TITLE: **ONLINE TRANSACTIONS IN THE LONG-TERM INSURANCE INDUSTRY**

DUE DATE: **13 APRIL 2006**

STUDENT NAME: **DANIEL STRYDOM GOUWS**

STUDENT NUMBER: **GWSDAN002**

SUPERVISOR: **PROF J HOFMAN**

Research dissertation presented for the approval of Senate in fulfilment of part of the requirements for the Master of Law in approved courses and a minor dissertation. The other part of the requirement for this qualification was the completion of a programme of courses.

I hereby declare that I have read and understood the regulations governing the submission of Master of Law dissertations, including those relating to length and plagiarism, as contained in the rules of this University, and that this dissertation conforms to those regulations.

Signature:.....

Summary

The long-term insurance industry is a heavily regulated industry, offering products that are often perceived to be complex in nature and not ideally suited for sale over the Internet. This paper will consider the extent to which our law currently allows for the sale of long-term insurance products through the electronic medium and identify the possible obstacles thereto. It will also point out potential solutions to such obstacles.

INDEX

CHAPTER I

INTRODUCTION: THE DIGITAL REVOLUTION AND e-COMMERCE

During the previous half century the world experienced the development of technology that brought about a revolution in the way that information could be exchanged and stored. By developing the technology that could transform information previously represented in analog format into a binary code, it became possible to communicate and store previously unthinkable quantities of data accurately and almost instantaneously. This phenomenon and the effect that it had on the world is generally referred to as the digital revolution.

Because of the tremendous impact that the ability to communicate and store these vast volumes of information has had on the way that people interact, especially with the advent of the Internet, the development has been likened to both the agricultural and industrial revolutions.[1] In discussing the impact of the Internet on society, Prof Julien Hofman in his work entitled *Cyberlaw – A guide for South Africans doing business online* comments that "*the information revolution brought about what was previously unimaginable: it conquers time and space as virtually any amount of information can now be sent almost anywhere in the world in the blink of an eye*."[2]

The technology underlying this revolution consisted of a series of technological breakthroughs that can be traced back to as early as 1837 when Samuel Morse developed the telegraph which could convert physical movement into electronic impulses that could then be transmitted along a telegraph cable. These electrical impulses were referred to as being "analog" because it could be represented as a series of sine waves, the modulation of which was "analogous" to fluctuations in the human voice or any other

[1] Hofman J, *Cyberlaw, a guide for South Africans doing business online,* Ampersand Press, 1999, Chapter 1 at page 12
[2] *Ibid* at page 13

sound being transmitted.[3] An important development thereafter was the ability to convert an analog source into digital data. The term "digital" which is Latin for "finger – counting on the fingers" refers to a system that uses binary numbers for the input, processing, transmission, storage, or display of data. Information is converted into either one of two electronic or optical pulses, logic 1 (pulse present) or 0 (pulse absent). In essence therefore, the digital revolution enabled signals (representing information) that was previously analog into a binary representation of ones and zeros.

A further important breakthrough was the development of the micro processor which made widespread availability and use of the personal computer possible with its rapidly increasing performance capabilities. Computer technology enabled various other mediums and devices such as cameras and music players to make use of this fantastic capability. With digital cameras, optical and video images can be recorded and stored digitally and transferred to any destination on the planet with virtually no loss of clarity or resolution. Similarly, audio recordings can by made and stored digitally allowing easy access to vast numbers of sound recordings, such as music collections.

Of particular importance was the development of the Internet and the worldwide web (the "WWW"). The WWW is a network of digital data bases and communication links connecting virtually the entire developed world. It opened, at a rapid pace, new avenues for communication and information sharing on a global scale. This new ability to communicate had a profound effect on the way that people interact and it was not long before it started to change the way that they do business. It soon became possible for providers of goods and services to market themselves and their products through this network and enter into transactions with clients in the same manner. Businesses are increasingly doing business with other businesses through the electronic medium ("B2B") and, with their clients ("B2C").

[3] http://searchsmb.techtarget.com/sDefinition/0,,sid44_gci211561,00.html (accessed : 11/04/06)

Research conducted in 2004[4] indicated that there were 580 million Internet users worldwide. It was forecast that this number would grow to 1.07 billion by 2005, 1.21 billion by 2006 and 1.35 billion by 2007. Revenues from B2C e-commerce worldwide were estimated to have grown from $59.7 billion in 2000 to $428.1 billion in 2004.[5] In the USA, sales figures published by the US Census Bureau indicated that US retail e-commerce sales during the third quarter of 2005 amounted to $20.8 billion[6]. This figure represented a growth of 26.7% as compared to the third quarter of 2004. Total retail sales increased only by 8.5% during the same period.

The above clearly illustrates the increase in Internet connectivity worldwide and the resultant and growing use thereof by businesses and their customers for business purposes.

In an article entitled "A Web Wake-Up Call"[7] the author quotes a study conducted by Limra in 2004 which indicated that approximately 40% of consumers who shop for life assurance do not have any face-to-face contact with an insurance professional. Limra is a worldwide association of insurance and financial services companies, established to help its members improve their marketing and distribution networks. It showed that the computer is increasingly the medium of choice for sophisticated buyers and although such buyers may not necessarily buy insurance online, the Internet can help shorten the decision-making process and increase buyers' product knowledge. The author concludes that "*traditional marketing methods such as mail, direct sales, telemarketing and broadcast media still work and should not be discounted"* and that "*consumer behaviour is changing, and consumers will be looking at , and purchasing from companies that have the information and products they want – when they want it"*.

---

[4] www.e-consultancy.com/publications/internet-stats-compendium (accessed : 10/04/06)
[5] www.emarketer.com; http://retailindustry.about.com/library/bl/bl_em0320.htm (accessed : 10/04/06)
[6] http://www.census.gov/mrts/www/ecomm.html (accessed : 10/04/06)
[7] Brett J, *A Web Wake-Up Call,* Limra's Market Facts Quarterly / Fall 2005

Because of the tremendous pace at which the digital revolution occurred and is still occurring as technology develops, the law did not always keep pace with the new ways of communicating and transacting . Prof Hofman[8] comments on this state of affairs by pointing out that the rule of law ideally develops in an incremental and organic manner as it is essentially based on an orderly development of legal principles. *"Given such a conservative predisposition"*, he states, *"the law is badly placed to deal with revolution. Revolution and the law are at opposite poles"*.

This paper will endeavour to consider the extent to which our legal system currently makes it possible for transactions to be concluded electronically within the long-term insurance and financial services industry.

[8] Hofman *op cit* page 14

CHAPTER II

CURRENT e-COMMERCE TRENDS IN SOUTH AFRICA AND THE SOUTH AFRICAN FINANCIAL SERVICES INDUSTRY

e-Commerce in the South African financial services industry is currently dominated by online banking services. Such services typically include:-

(a) Balance enquiries;
(b) Account payments;
(c) Fund transfers;
(d) Inter-account transfers
(e) Checking interest rates
(f) Information requests
(g) Stop Orders
(h) Cheque book ordering
(i) Credit Card applications/ordering
(j) Mortgage bond applications
(k) Financial calculators
(l) Personal loan applications
(m) Car finance applications
(n) Home loan applications
(o) Purchasing foreign exchange.

Other e-finance services include online share trading, online unit trust purchasing and online insurance purchasing. Research conducted by BMI-TK Group, 2002 indicated an overall growth of the e-financial services market of 35% between 2000 and 2001. It forecasted an average growth of 20% between 2001 and 2006. A total amount of R798m in transaction fees were generated from electronic banking in 2001. This was estimated to

grow to R1.9b by 2006. Total online financial services Internet usage was expected to increase in value terms from R730 000.00 in 2000 and R123.6m by 2006.

The Long-term Insurance industry

Long-term insurance, as opposed to short-term insurance, refers to "*the business of providing …… policy benefits under long-term policies*"[9]. A long-term policy is defined in the Long-term Insurance Act, 52 of 1998 ("the LTIA") as "*an assistance policy, a disability policy, fund policy, health policy, life policy or sinking fund policy, or a contract comprising a combination of any of those policies*".

To be able to market and sell such policies, an assurer must be registered as a long-term assurer in terms of the LTIA. There are currently 77 companies registered as long-term assurers in South Africa[10]. Most long-term assurers offer policies to customers generally providing for the following benefits:-

- Life insurance (term or whole life);
- Disability insurance (occupational disability);
- Health benefits (pays benefits upon the occurrence of a "health event" or illness).

Normally, the policies also provide for the long-term saving of funds, and are therefore ideal vehicles to save for retirement. The long-term assurers enjoy a virtual monopoly of the pension funds saving industry, by virtue of the fact that life and disability benefits can be offered to a client whilst such client is also saving for retirement. Most life assurers therefore established pension funds for this purpose, whilst their asset management divisions are tasked to invest the combined savings of policyholders with the view to ensuring the best possible returns for policyholders upon disability or retirement. Apart from contributing towards pension funds, policyholders

[9] The Long-term Insurance Act, 52 of 1998
[10] www.fsb.co.za (accessed on 10/04/06)

also invest in normal savings funds and investments, i.e. as long as the savings vehicle is underwritten or "wrapped" in a long-term policy. A typical long-term assurer will therefore offer products that are designed to cater for the abovementioned needs. Examples of such products are the following:-

- Life insurance policies;
- Disability insurance policies;
- Pension fund policies;
- Endowment (investment) policies;
- Employment benefits policies.

Many assurers will also offer medical aid scheme benefits, but such benefits are regulated by the Medical Schemes Act and not in terms of the LTIA. It therefore falls outside of the ambit of the long-term insurance business for purposes of this paper.

Other important facets of the industry comprise:

- Marketing (the offering of products and services and providing information);
- Rendering Advice (relating to the products and services available);
- Underwriting;
- Contracting, including amendments/endorsements during the continuation of a policy or product;
- Claims processing.

The policies referred to above are marketed and sold to individual policyholders, but policies offering employee benefits are made available to corporate entities or small and medium to large employers who can negotiate with long-term assurers for the provision of life, disability and pension benefits to their employees as a group. In such a case a single policy agreement with a long-term assurer can for example provide life and disability benefits to all employees of the entity. Policy benefits are thereby made

available to the entities' employees as part of their benefits of employment, known as fund policies.

Distribution Channels

Most long-term assurers rely heavily, if not entirely, on intermediaries as the preferred distribution channel for the sale of its products. Such intermediaries can be employees of the assurer i.e. "*tied agents*" or independent brokers, who function independently of any single life assurer and who can therefore decide which life assurer's product to procure for their clients. The "*tied agent*" would normally only sell the products of his or her employer. In both cases, the intermediaries are remunerated on a commission basis although the "*tied agent*" will generally also receive a basic retainer. In the case of independent brokers, each long-term assurer would enter into agreements with as many brokers as possible whereby such broker would be offered commission on policies purchased from the assurer for each of the broker's clients.

Most long-term assurers also offer its products for sale directly to the consumer through Direct Marketing initiatives. As stated, this paper will consider the extent to which long-term insurance policies can be purchased through the Internet. It follows that such transactions will not involve an intermediary and will most likely be offered through direct marketing divisions or e-Commerce business units. It will be shown below that the regulatory requirements differ in certain important respects, depending on whether policies are sold *via* intermediaries or directly, as in the case of an online transaction.

Industry Regulation - The Long-term Insurance Act

The life insurance industry is generally regarded as a heavily regulated industry. Reference has already been made to the fact that life assurers must be registered in terms of the LTIA. The LTIA contains various provisions that apply to the business practices

and product offerings of long-term assurers. Chapter VII of the LTIA for instance, contains provisions applicable to business practices, policies and policyholder protection. The so-called "Policyholder Protection Rules"[11] were published by the Minister of Finance in terms of s. 62 of LTIA and contain provisions applicable to the marketing and sale of long-term insurance policies.

PART VII of the Act deals with business practices and "policyholder protection" to which long-term assurers must adhere when selling these products. S. 44 of the Act, requires a policyholder to be provided with a "*free choice in certain circumstances*". This requires the "*policyholder to be given written notification of free choice*" where a policy is taken out or ceded in terms of an agreement of loan or where credit is granted. In terms of sub-section (2) the said requirement "shall be deemed not to have been complied with" if the policyholder has not "confirmed in writing" that he or she:

> *"(a) was given prior written notification of his or her entitlement to the freedom of choice referred to in that subsection;*
> *(b) exercised that freedom of choice; and*
> *(c) was not subject to any coercion or inducement as to the manner in which he or she exercised that freedom of choice."*

In terms of s. 48 of the Act a person who enters into a long-term policy must, as soon as possible, but not later than 60 days after the transaction, be provided with a written summary of:

> *"(a) those of the representations made by or on behalf of that person to the assurer which were regarded by that assurer as material to its assessment of the risks under the policy;*
> *(b) the premiums payable and the policy benefits to be provided under the policy; and*
> *(c) the events in respect of which the policy benefits are to be provided and the circumstances (if any) in which those benefits are not to be provided."*

[11] Government Gazette, GN 26854, 30 Sept 2004.

Such summary may be provided to the client in electronic form, as stated in s. 12 of the Electronic Communications and Transactions Act, 25 of 2002 (the "ECT Act")[12].

The Policyholder Protection Rules were formulated with the objective "*to ensure that policies…are entered into, executed and enforced in accordance with sound insurance principles and practice in the interests of the parties and in the public interest*". It contains provisions that apply specifically to "direct marketers". It is interesting to note, at this stage, that the Rules define "direct marketing" as "*the marketing of a policy by way of telephone, Internet, media insert, direct or electronic mail in a manner which includes the required transaction requirement pertaining thereto…*" and a "direct marketer" as "*an assurer who, in the normal course of business, carries on business in the form of direct marketing*". The legislator clearly envisaged in the drafting and promulgation of the Rules, the selling of long-term insurance policies through the electronic medium and careful consideration must therefore be given to the provisions in this regard. It will be shown in the discussion of the FAIS Act below, that similar mention is made to "direct marketing".

Part III of the Rules that deal with the requirements applicable to direct marketers states in Rule 4.4 thereof that "*a provision of a Rule in this Part is not applicable to a direct marketer in any case where a compliance duty in respect of the same matter is imposed on the direct marketer by, in terms of or by virtue of any other law*". Any long-term assurer who offers long-term insurance policies for sale through the electronic medium, will therefore have to ensure that it is compliant not only with the provisions of the FAIS Act[13] discussed below, but also with any provisions contained in these Rules that is perhaps not contained in the FAIS Act.

[12] Sec. 12 of the ECT Act states that a requirement in law that a document or information must be in writing is met if the document or information is (a) in the form of a data message and (b) accessible in a manner usable for subsequent reference.
[13] Financial Advisory and Intermediary Services Act, No 37 of 2002

Part V of the Rules contains provisions applicable to cancellations of policies and cooling off periods. In terms of Rule 6.1 a policyholder may "*in any case where no benefit has yet been paid or claimed or an event insured against has not yet occurred*" cancel the policy taken out, provided that it is done within 30 days of receipt of the summary issued in terms of s 48, referred to above.

The Financial Advisory and Intermediary Services Act

A further and very important Act that regulates the selling of long-term insurance policies and the rendering of financial advice is the Financial Advisory and Intermediary Services Act, No. 37 of 2002 ("FAIS"). This Act was promulgated to "*regulate the rendering of certain financial advisory and intermediary services"* and came into effect on 31 October 2004. It applies to all providers of financial services, which by definition includes long-term assurers. It contains detailed provisions relating *inter alia* to:-

(a) The licensing of all financial services providers (s 7);
(b) The qualifications and training of representatives of financial services providers (ss 13-14);
(c) The responsibility of financial services providers to ensure compliance with the Act (s 17);
(d) Record keeping (s 18);
(e) Interaction with clients and compulsory disclosures as well as the rendering of advice (ss 3 and 6 of the General Code, ito s 15 of the Act).

It is important for purposes of this paper, to carefully consider the definition of certain terms contained in the Act as it has an important bearing on the selling of long-term insurance policies through the electronic medium. In terms of the Act a "financial services provider" or "FSP" means "*any person…who as a regular feature of the business of such person-*

(a) furnishes advice; or

(b) furnishes advice and renders any intermediary service; or

(c) renders an intermediary service".

"Advice" is defined in the Act as:

"*any recommendation, guidance or proposal of a financial nature furnished, by any means or medium, to any client or group of clients—*

(a) in respect of the purchase of any financial product; or

(b) in respect of the investment in any financial product; or

(c) on the conclusion of any other transaction, including a loan or cession, aimed at the incurring of any liability or the acquisition of any right or benefit in respect of any financial product; or

(d) on the variation of any term or condition applying to a financial product, on the replacement of any such product, or on the termination of any purchase of or investment in any such product,

and irrespective of whether or not such advice—

(i) is furnished in the course of or incidental to financial planning in connection with the affairs of the client; or

(ii) results in any such purchase, investment, transaction, variation, replacement or termination, as the case may be, being effected."

A similarly wide definition applies to "intermediary service" which is defined as:

"*any act other than the furnishing of advice, performed by a person for or on behalf of a client or product supplier—*

(a) the result of which is that a client may enter into, offers to enter into or enters into any transaction in respect of a financial product with a product supplier; or

(b) with a view to—

(i) buying, selling or otherwise dealing in (whether on a discretionary or non-discretionary basis), managing, administering, keeping in safe custody, maintaining or servicing a financial product purchased by a client from a product supplier or in which the client has invested;

(ii) collecting or accounting for premiums or other moneys payable by the client to a product supplier in respect of a financial product; or

(iii)receiving, submitting or processing the claims of a client against a product supplier".

Also of importance is the express exclusion contained in s 1(3)(a) which states that, for purposes of the Act, "advice" does not include:

"*(i) factual advice given merely—*

(aa) on the procedure for entering into a transaction in respect of any financial product;

(bb) in relation to the description of a financial product;

(cc) in answer to routine administrative queries;

(dd) in the form of objective information about a particular financial product; or

(ee) by the display or distribution of promotional material;

(ii) an analysis or report on a financial product without any express or implied recommendation, guidance or proposal that any particular transaction in respect of the product is appropriate to the particular investment objectives, financial situation or particular needs of a client".

A General Code of Conduct for authorised financial services providers and representatives was published in terms of s. 15 of the Act, which Code contains equally detailed provisions relating to:-

(a) The disclosure of information in respect to product suppliers (s 4);

(b) The furnishing of advice (s 8);

(c) Advertising and direct marketing (s 14); and

(d) Complaints resolution (s 15).

The Code defines "*direct marketing"* as "*the rendering of financial services by way of telephone, Internet, media insert, direct mail, or electronic mail …"* and

"writing" as including *"communication by telefax or any appropriate electronic medium…"*. It will clearly apply to the selling of long-term insurance policies through the electronic medium. It was pointed out above that "the rendering of financial services" involves the rendering of advice or the rendering of an intermediary service or a combination of the two. The definition of "direct marketers" in the Code is important, as it distinguishes by implication between the rendering of financial services in the "normal course of business" and the rendering of financial services by way of direct marketing. Where the services are rendered in the "normal course of business" the provisions contained in Parts III, IV, VI and VII must be complied with. Parts III, IV, VI and VII each refer to "*a provider other than a direct marketer*".

If, however, the services are rendered by way of direct marketing, the provisions contained in Part X applies. It provides, as is the case in Parts III, IV, VI and VII, for the furnishing of information on the product supplier, information on the FSP, information about the financial service rendered (the product) and the manner in which advice must be rendered.

Part X of the General Code, and in particular Paragraph 15 thereof, contains the requirements that will be applicable to a direct marketer when it offers the sale of long-term insurance policies through the Internet. It therefore has direct relevance to the topic of this paper. Paragraph 15 states that a direct marketer must "*at the earliest reasonable opportunity*" furnish a client with the following information:

> *"(a) The business or trade name of the direct marketer;*
> *(b) confirmation whether the direct marketer is a licensed financial service provider and details of the financial services which the direct marketer is authorised to provide in terms of the relevant license and any conditions or restrictions applicable thereto;*
> *(c) telephone contact details of direct marketer (unless the contact was initiated by the client);*
> *(d) telephone contact details of the compliance department of the direct marketer;*
> *(e) whether the direct marketer holds professional and indemnity insurance."*

Paragraph 15(2) contains requirements that must be met when "*when providing a client with advice in respect of a product*". By implication, a direct marketer will therefore not always or necessarily enter the arena of "giving advice" when it renders a financial service, even if it includes entering into a transaction with a client. As pointed out above, that "advice" does not include mere factual information about a product or the procedure to be followed when entering into a transaction in respect thereof. It is submitted that a long-term assurer that sells long-term insurance policies through the Internet, will in certain instances be able to sell long-term insurance policies without also providing advice, as defined. If a client however requires advice before entering into a transaction or at any stage during the process, it is argued that such advice can be rendered through the Internet whilst maintaining compliance with the Code. In this regard Paragraph 15(2) states that, where advice is furnished, a direct marketer must "*make enquiries to establish whether the financial product or products concerned will be appropriate, regard being had to the client's risk profile and financial needs, and circumstances*." It is entirely possible to obtain such information from the client electronically.

Part II of the Code contains "General Provisions" applicable to FSP's. It contains detailed provisions applicable to "*representations made and information provided to a client by a provider*". Included in the provisions are the following:

> *"Representations made and information provided to a client by the provider—*
>
> *(i) must be factually correct;*
> *(ii) must be provided in plain language, avoid uncertainty or confusion and not be misleading;*
> *(iii) must be adequate and appropriate in the circumstances of the particular financial service, taking into account the factually established or reasonably assumed level of knowledge of the client;*
> *(iv) must be provided timeously so as to afford the client reasonably sufficient time to make an informed decision about the proposed transaction;*
> *(v) may, subject to the provisions of this Code, be provided orally and, at the client's request, confirmed in writing within a reasonable time after such request;*

(vi) must, where provided in writing or by means of standard forms or format, be in a clear and readable print size, spacing and format;

(vii) must, as regards all amounts, sums, values, charges, fees, remuneration or monetary obligations mentioned or referred to therein and payable to the product supplier or the provider, be reflected in specific monetary terms: Provided that where any such amount, sum, value, charge, fee, remuneration or monetary obligation is not reasonably pre-determinable, its basis of calculation must be adequately described; and

(viii) need not be duplicated or repeated to the same client unless material or significant changes affecting that client occur, or the relevant financial service renders it necessary, in which case a disclosure of the changes to the client must be made without delay".

Policing compliance: the Financial Services Board

Compliance and adherence to both the LTI and FAIS Acts is policed by the Financial Services Board ("FSB") established in terms of the Financial Services Board Act 97 of 1990. In terms of s 3(a) of the FSB Act it is the duty of the FSB *"to supervise the compliance with laws regulating financial institutions and the provision of financial services"*. All providers of financial services must report annually to the FSB on their compliance with the abovementioned legislation and any business procedure that offers online selling of long-term insurance products will therefore have to be included in such reporting. Non-compliance with the abovementioned legislation could have grave consequences for a financial services provider as it could ultimately lead to the withdrawal of its authorisation or licence.

In an article that appeared in the "New South Wales Society for Computers and the Law Journal",[14] Charles Schofield and Henry Davis York discuss the impacts of the Financial Services Reform ("FSR") that came into force in Australia during March 2004. They point out that financial institutions are *"heavy users of technology"* and that the FSR regime could have a broad impact on their information technology systems. They

[14] Schofield S and Davis York H, *FSR Impacts on Financial Services Technology*, New South Wales Society for Computers and the Law, Journal: December 2004, Issue 58

highlight the areas of expected impact as licensing (the licence to operate), disclosure and conduct. After pointing out the various disclosure requirements that apply to the provision of financial services in Australia, they state:

> *"These disclosure obligations, in the context of financial services technology, have the greatest impact on the online delivery of financial services. Organisations providing financial products online, for example, need to ensure that their IT systems are capable of delivering an up to date product disclosure statement to the customer at or before the time the product is offered or issued to the customer"*.

They also warn that organisations must be able to prove what disclosures were made to the customer or customers should it ever be called into question. They emphasise the importance of the capability of IT systems of recording disclosures and that *"systems need to be tested regularly to demonstrate that they are providing disclosure when required, and testing results need to be retained for future proof, if needed"*. According to Schofield and York, IT systems can also be used to *"prompt complaint behaviour"*. By this they mean that software can be used to issue an "*automated prompt"*. The system can be programmed to require acknowledgment from the client that advice has been given before processing a transaction. This can provide an audit trail to the financial services provider whereby it can monitor and demonstrate its compliance to regulatory requirements.

The Life Offices Association of South Africa

The Life Offices Association of South Africa (the "LOA") is a voluntary association formed by long-term insurance companies doing business in South Africa. Its objectives are to "*promote a better understanding of life insurance among the general population of the country, represent the industry and its policyholders in negotiations with the authorities and [to] regulate their industry*". Through the LOA, the industry regulates

itself voluntarily by adherence to several Codes of Conduct[15]. These Codes deal with various aspects of the long-term insurance industry, and includes *inter alia* Codes such as:

- the Code on the Maintenance of the Life Register
- the Code on the Demarcation of Health Insurance an Medical Schemes business
- the Code on Good Practice for Disability Insurance
- the Code on Medical Requirements, Medical Report forms and related matters
- the Code on the Replacement of Policies.

Several of the Codes contain provisions that will have to be borne in mind when offering long-term insurance policies for sale through the Internet. Examples of such provisions are:

- Paragraph 4 of the Code on the Life Register that requires life assurers to inform the LOA of "*any written applications for new policies*". Member offices are required by Paragraph 8 of the Code to obtain a signed "*authorisation*" from an applicant whereby medical information relating to the application may be shared with other assurers;
- In terms of the Code on Medical Requirements, standard medical report forms and declarations must be used by all life assurers; and
- The Code on Replacements aims to prevent the potentially harmful practice of advising clients to replace existing policies with new policies. The risk that is being regulated is of an intermediary recommending new products not strictly in the interests of the client but in order to generate fresh commission. The Code therefore states as its "basic rule" the following:

> "*The basic rule is that when a proposal is sought or received in respect of any policy or variation of a policy, it is the duty of the intermediary (and, in respect of direct marketing by a member office, the duty of the member office) to establish whether such policy or variation is a replacement policy, and if*

[15] www.loa.co.za

> *so to ensure that the client is properly counseled as required by this Code, PPR and/or FAIS on the consequences of a replacement and is enabled to take the decision to replace on a fully informed basis*."

From the above it is clear that a long-term assurer that sells policies through the Internet, will have to ensure that all the necessary disclosures are made and information and declarations are obtained from a client, as prescribed by the FAIS- and LTI Acts as well as the various Codes of Conduct applicable to the business. Discussed below are the various techniques that can be used on a website to bring information to the attention of a client and how to prove that the client has applied his or her mind thereto and, where necessary, that he or she has agreed to particular terms, before proceeding with an online transaction[16].

Other legislation: The Financial Intelligence Centre Act, 38 of 2001

The Financial Intelligence Centre Act, 2 of 2000 ("FICA") was promulgated essentially to combat money-laundering activities. It established a Financial Intelligence Centre ("FIC") whose duty it is "*to make information collected by it available to investigating authorities*". It furthermore forces "*accountable institutions*" to obtain and store certain fields of information about their clients, before entering into transactions with them. Such information relates *inter alia* to the client's identity, physical address and source of funds. The information must not only be obtained, but also verified. Any "suspicious transactions", as defined, must be reported to the FIC.

Included in the list of "accountable institutions" are long-term assurers. A long-term assurer may therefore not enter into a long-term insurance contract with a client, before first identifying and verifying the identity of such client. Not all transactions are however "reportable" in terms of the Act. The Regulations to the Act contain the following important exemptions:

[16] Pages 30 and 31

"*(a) any long term insurance policy which is a fund policy or a fund member policy as defined in the Long-term Insurance Act, 1998 and the regulations thereto and in respect of which the policyholder is a pension fund, provident fund or retirement annuity fund approved in terms of the Income Tax Act, 1962;*

(b) ……;

(c) ……;

(d) ……;

(e) ……;

(f) any long term insurance policy which provides benefits only upon the death, disability, sickness or injury of the life insured under the policy;

(g) any long-term insurance policy in respect of which recurring premiums are paid which will amount to an annual total not exceeding R25 000,00, subject to the condition that the provisions of Parts 1 and 2 of Chapter 3 of the Act have to be complied with in respect of every client—

(i) who increases the recurring premiums so that the amount of R25 000,00 is exceeded;

(ii)who surrenders such a policy within three years after its commencement; or

(iii)to whom that accountable institution grants a loan or extends credit against the security of such a policy within three years after its commencement;

(h) any long term insurance policy in respect of which a single premium not exceeding R50 000,00 is payable, subject to the condition that the provisions of Parts 1 and 2 of Chapter 3 of the Act have to be complied with in respect of every client—

(i) who surrenders such a policy within three years after its commencement; or

(ii) to whom that accountable institution grants a loan or extends credit against the security of such a policy within three years after its commencement;

(i) ……;

(j) ……;

(k) any other long term insurance policy on condition that within the first three years after the commencement of the policy the surrender value of the policy does not exceed twenty per cent of the value of the premiums paid in respect of that policy."

Where a long-term assurer wishes to enter, over the Internet, into a transaction for the sale of a policy that does *not* fall within the exemptions, particular care will have to be taken to comply with the Act. Careful consideration will have to be given to the extent to which an accountable institution is required to identify and verify the identity of a prospective client. In terms of Regulation 3 an accountable institution must obtain from a client his or her full names, date of birth, identity number and residential address. This information must be verified by "*comparing these particulars with …an identification document of that person…or another document issued to that person…which …bears…a photograph of that person…*". The residential address must be verified "*by comparing these particulars with information which can reasonably be expected to achieve such verification and is obtained by reasonably practical means*". It is generally accepted that verification can be obtained by requiring a prospective client to produce his or her bar-coded ID book which is then perused to verify the person's full names, identity number and date of birth. The client is then expected to produce any one of a variety of documents that would verify his or her residential address, such as a utilities bill, municipal rates and taxes invoice or telephone account.

Such verification can logically only occur when the transaction takes place in a so-called “face-to-face” situation. The question is therefore how to establish and verify a client’s identity and residential particulars in a “non face-to-face” transaction as envisaged by a transaction over the Internet. Regulation 18 deals with “v*erification in absence of contact person”* and provides as follows:

> “*If an accountable institution obtained information in terms of these regulations about a natural or legal person, partnership or trust without contact in person with that natural person, or with a representative of that legal person or trust, the institution must take reasonable steps to establish the existence or to establish or verify the identity of that natural or legal person, partnership or trust, taking into account any guidance notes concerning the verification of identities which may apply to that institution.*”

It is submitted that a client’s identity can thus be established by obtaining a faxed copy of his or her identity document and by verifying it by comparing it to the records of the Department of Home Affairs or any other records held by a independent third party such as a national credit bureau. Regulation 18 does not mention the verification of a person’s residential address but it is submitted that this is a mere oversight and that the residential address may similarly be verified by an independent third party such as a local municipality.

It is clear, at least, that it was the intention of the legislature, in enacting Regulation 18, to allow for transactions that are conducted in a non face-to-face situation such as over the Internet. It is regrettable that the legislator did not give a clearer indication of how such verification may take place as there could be those that argue that strict rules should apply to non face-to-face transactions due to the increased risk of criminal abuse.

Such stricter rules in case of non face-to-face transactions could represent an obstacle to online transacting in the long-term insurance industry.

It is interesting to note that the Australian Financial Transactions Reports Act of 1988 which also requires the identification and verification of clients for purposes of combating money laundering; and that certain original documents must be produced; and for the client to sign in the presence of the party keeping the reference or undertaking verification. In an article dealing with proposed changes to the Australian Uniformed Consumer Credit Code[17], the authors considered proposed changes to the Australian Uniform Consumer Credit Code which would enable credit contracts to be formed electronically and for documents and notices related thereto to be given electronically.

They regard the Financial Transaction Reports Act as a *"major legislature obstacle to transacting with a customer solely by electronic means"*. They also point out that expected changes to the Australian money laundering legislation to bring it in alignment with the recommendations of the International Financial Action Task Force on Money Laundering dated June 2003, could require a higher standard of customer due diligence obligations to be adhered to. They warn that it is *"at this stage it is difficult to predict to what extent this will hinder the ability of lenders to transact electronically with customers"*. A similar process of tightening client identification and verification requirements might also occur in South Africa as our FIC Act was also drafted with the Financial Action Task Force Principles as a guideline. As in Australia, it is therefore to be seen to what extent anti money laundering provision would future hinder the ability of long-term assurers to transact electronically with clients.

[17] Lodge T and Kho R, *Online Transactions between Members and Borrowers – Proposed Changes to the Uniformed Consumer Credit Code*, New South Wales Society for Computer and the Law Journal : December 2004, Issue 58

CHAPTER III

REGULATION OF ELECTRONIC TRANSACTIONS AND COMMUNICATIONS IN SOUTH AFRICA

Long-term assurers who wish to sell their products online will have to study the provisions contained in the Electronic Communications and Transactions Act, No. 25 of 2002 ("the ECT Act") carefully, as the Act applies to almost all online activity. The Act applies not only to websites that allow transactions to be performed online, but also where they merely provide information. It also applies to the use of electronic communications where those communications are intended to have legal consequences. This Chapter will therefore study the various provisions contained in the ECT Act, in as far as they would apply to the online selling of long-term insurance products.

The Electronic Communications and Transactions Act, No. 25 of 2002

The ECT Act was promulgated on 31 July 2002 and took effect by Proclamation on 30 August 2002. The Act was drafted and passed by Parliament to regulate various aspects relating to electronic communications and transactions. S 2 of the Act which deals with its objects, confirm that it was promulgated *"to enable and facilitate electronic communications and transactions in the public interest"*. The section contains a list of various objectives that the Act aims to achieve in support of the mentioned main object, which includes *inter alia*:-

> *"(a) recognise the importance of the information economy for the economic and social prosperity of the Republic;*
> *(b) ……..*
> *(c) promote the understanding and, acceptance of and growth in the number of electronic transactions in the Republic;*

(d) remove and prevent barriers to electronic communications and transactions in the Republic;
(e) promote legal certainty and confidence in respect of electronic communications and transactions;
(f) ……
(g) ……..
(h) ensure that electronic transactions in the Republic conform to the highest international standards;
(i) ……..
(j) develop a safe, secure and effective environment for the consumer, business and the government to conduct an use electronic transactions;
(k) promote the development of electronic transactions services which are responsive to the needs of users and consumers."

The Act also contains various provisions aimed at promoting a sound national e-strategy for the Republic of South Africa intended to promote universal access to electronic communications and transactions and maximise the benefits of electronic transactions including provision of the services to the historically disadvantaged persons and communities of South Africa. It must also promote the development of human resources within a suitable national e-strategy and the development of processes, programmes and infrastructure through which SMME's can benefit.

Of particular importance for the purposes of this paper is Chapter III of the Act which deals with electronic transactions. The Chapter "*enables*" electronic transactions by giving legal recognition to data messages. The various sections of the Chapter and their importance to online transactions will be discussed below.

It is necessary to note that most of the provisions contained in Chapter III of the Act follow the wording of the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce[18] which was adopted in 1996. The Commission was established by the General Assembly of the United Nations to work towards harmonisation and unification of the Law of International Trade. The Model Law on Electronic Commerce is intended "*to facilitate the use of modern means of*

[18] www.uncitral.org/uncitral/en/uncitral-texts/electronic_commerce/1996Model.html (accessed 15/02/06)

communications and storage of information". The Model Law relies heavily on the so-called *doctrine of functional equivalence*. In terms of this doctrine or approach, rules must be formulated to ensure that the electronic media provides a functional equivalent for paper-based concepts such as "*writing*", "*signature*" and "*original*". These aspects play an important role in the formation of agreements and therefore in the world of commerce. As more and more commercial transactions are conducted through the electronic medium, it becomes more and more important for the Law to provide certainty in respect of such transactions. The fact that the communications and transactions are conducted through the electronic medium means by implication that the traditional "*paper contracts*" and "*signatures*" are no longer available to provide certainty in respect of the many issues arising out of commercial agreements. The Model Law therefore aims to provide standards by which the legal value to be attached to electronic messages can be assessed. The intention is that all Member States should "*give favourable consideration to the Model Law when they enact or revise their laws in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information."*[19] As stated above, much of the wording of Chapter III of the ECT Act follows the wording contained in the Model Law.

Legal recognition of data messages

S 11(1) of the Act can, in many respects, be regarded as the key to the legal recognition of electronic transactions. The section gives legal recognition to "*data messages"* which is defined in the Act as "*data generated, sent, received or stored by electronic means"*.[20] It includes voice messages where it is used in an automated transaction and stored data. In terms of s. 11(1), data messages are given legal recognition by stating that "*information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message"*. This key provision makes it possible for parties to a transaction to rely on information pertaining to the

[19] Resolution adopted by the General Assembly of the United Nations Resolution 51/162 of 16 December 1996
[20] Sec 1 of the ECT Act

transaction regardless of the fact that it does not exist on paper, as was traditionally the case, but exists only in electronic form. Previously, a party to a contract wishing to rely on information which only exists in electronic form could have found it difficult if not impossible to prove that such information must be given legal recognition.

"Incorporation by reference"

S 11(2) states that information merely referred to in a data message enjoys the same treatment. This sub-section refers to the doctrine of *incorporation by reference* found in our Contract Law. In terms of this doctrine a contract can refer to information or legal implications not contained in the contract itself, but contained in a separate document or location. Although it is therefore not contained in the agreement itself, it will still have legal effect and relevance to the agreement. Numerous disclosures that must be made to a prospective policyholder were listed in Chapter II above. The electronic medium is ideally suited to referring a prospective client to various Codes, Regulations and stipulations which must be brought to his or her attention during the course of an electronic transaction. Such disclosures and information can be "*incorporated by reference"* by making use of various methods provided by the electronic medium such as click-wrap and web-wrap functionality.

Current technology provides for at least three ways of bringing information referred to, to the attention of a person conducting a transaction on a web-site. All three methods make use of the so-called "*hyperlink*". A "*hyperlink*" is a "*shortcut"* to other documents embedded in the text of an HTML document. The reader of the HTML document does not have to type in the address of the other document in order to visit and read it. When a cursor is moved over such hyperlink it "*shows up"* or "*changes"* so as to alert the reader of its existence.

A hyperlink may, firstly, be in the form merely as a reference at the bottom of a page. The reader will of own volition have to enter the link if interested. This form is

referred to as *"browse-wrap"*. A second method is to require the reader to click on the words *"I agree"* before being allowed to proceed with the transaction. This is referred to as *"click-wrap"* and does not check whether the reader has in fact entered the other document. The third method actually displays the full content of the other document and requires the reader to click the words *"I agree"* or *"accept"* before being able to proceed with the transaction. This method is often referred to as *"web-wrap"*. It is submitted that financial services providers will have to consider the stricter forms of hyperlink such as the *"click-wrap"* or *"web-wrap"* methods if it wishes to satisfy itself and the regulatory authorities that it is compliant with the various requirement of disclosure referred to in this paper. A service provider will have to prove that the disclosures were indeed made to the client in such a way that he could not have continued with the transaction without applying his or her mind to the relevant information contained in the disclosure.

In the United States case of *Caspi v The Microsoft Network, LLC*[21], the Superior Court of New Jersey Appellate Division gave consideration to the validity and enforceability of a forum selection clause contained in an online subscriber agreement of the Microsoft Network (MSN), an online computer service. When a client applied to become a member of the service, the web-site through which the transaction was concluded would prompt such applicant to view multiple computer screens of information which included a membership agreement containing the clause in dispute. The person would only be able to complete registration after clicking *"I agree"* as to the terms of the agreement. It was argued that the clause in question was essentially *"hidden in the fine print"*. The court however came to the conclusion that *"there was nothing extraordinary about the size or placement of the forum selection clause text"* and that it was in the same format as the other provisions of the contract. The court concluded that the complainant *"must be taken to have known that they were entering into a contract and no good purpose, consonant with the dictates of reasonable reliability in commerce, would be served by permitting them to disavow particular provisions or the contract as a whole"*.

[21] *Caspi v The Microsoft Network L.L.C.* Superior Court of New Jersey Appellate Division 323 N.J. Super.118; 732 A.2d 528; 1999 N.J.Super. Lexis 254 (July 2, 1999)

The following was also said in the case of *Specht v Netscape Communications Corp.*[22]*: "Whether governed by the common-law or by Article 2 of the Uniform Commercial Code (UCC), a transaction, in order to be a contract, requires a manifestation of agreement between the parties…….. a consumer's clicking on a download button does not communicate as sent to contractual terms if the offer did not make clear to the consumer that clicking on the download button would signify as sent to those terms."* On the facts of the case, the court found that *"a reference to the existence of licensed terms on a sub-merged screen is not sufficient to place consumers on enquiry with constructive notice of those terms. Internet users may have, as defendants put it, 'as much time as they need' to scroll through multiple screens on a web-page, but there is no reason to assume to that viewers will scroll down to subsequent screens simply because screens are there. When products are 'free' and users are invited to download them in the absence of reasonably conspicuous notice that they are about to bind themselves to contract terms, the transactional circumstances cannot be fully analogized to those in the paper world of arms-length bargaining"*.

It is submitted that the courts in both cases referred to clearly applied the underlying and traditional principles of contract formation, which includes the forming of a proper consensus as to all the material terms that would apply to an agreement. Whatever method is used by long-term assurers offering transaction on a web-site, it should ensure that all material terms of the agreement as well as the various disclosures required by applicable legislation are properly brought under the attention of the client.

Equally, key to the enablement of electronic transactions is the provision contained in s 12 of the Act that any requirement in Law that a document or information must be in writing will be met if it is in the form of a data message. The data message must for obvious reasons be "*accessible in the manner usable for subsequent reference"*.

---

[22] *Specht v Netscape Communications Corp*, 306 F.3D17 (2d CIR. 2002)

Our law does not require a long-term insurance contract to be in writing, as in the case of agreement of sales in respect of immovable property. Reference was made above[23] to s 48 of the Long-term Insurance Act that requires the assurer to provide a policyholder with a "*written summary*" of a long-term policy not later than 60 days after the transaction. S 48 is therefore such a "*requirement in law*" referred to in s 12 and the summary can be provided to the policyholder in the form of a data message which must be "*accessible in a manner usable for subsequent reference*". The summary document can therefore be provided to the client in electronic form.

Electronic signatures and encryption

S 13 of the Act deals with electronic signatures. It is important to understand that the term "*electronic signature*" or "*digital signatures*" does not refer to a "*digital image*" or "*scanned version*" of a person's handwritten or even typed signature. It is rather an electronic identifier[24] that utilises cryptography measures which ensures the integrity and authenticity of information linked to the identifier, or "*signature*". To fully understand the concept of a digital signature it is first necessary to understand encryption and the role that it plays (and benefits that it brings) in the electronic media.

Data messages sent electronically over the Internet are normally sent in the form of "*plain text*". Sending it over the Internet in this form can be described as the equivalent of sending "*electronic post cards*" which can be read by any person who receives or intercepts the message. Where the sender of such a message does not wish it to be read by the wrong party, for instance where confidential personal or banking information is exchanged over the Internet during the course of an electronic transaction, encryption technology can be used to encode the information. This is called encryption. The technology underlying encryption consists basically of two components, being an

[23] Page 12
[24] Buys R et al, *Cyberlaw@SA II, The law of the Internet in South Africa,* Van Schaik, 2004, page 132

algorithm and a key. Algorithms are complex mathematical processes whereas the key is needed to "*unlock*" an encrypted message. In some instances the same key is used for both the encryption process and decryption. In other methods, different keys are used to encrypt and to decrypt.[25] Currently, technology provides for three methods of cryptography being "*secret key cryptography*", "*public key cryptography*" and "*quantum cryptography keys*". Secret key cryptography is used where the same key is used by the different parties to an electronic communication where public key cryptography utilises a system where two keys are used, one which remains private and one which is made public. It follows that both keys are required to decrypt an encoded message and confidentiality is therefore ensured for as long as the private key remains safe. Most online banking transactions are protected by this form of encryption. The bank holds and protects the private key whilst the public key is provided to customers. The "coding" of data messages in this manner is also referred to as *Secure Sockets Layer* or "SSL". Many websites use this protocol to exchange confidential information.[26]

Quantum cryptography keys refers to the use of photons or light particles for the encryption of data messages, rather than mathematical algorithms. Any interference with the photons or light particles alters its quantum properties which alerts the parties to the communication that the transmission was not secure. The photons are not used for the carrying of the actual message, but rather for the transfer of the cryptographic key.

The fact that data messages can be encoded in this manner has the following benefits:-

- Authentication: It makes it possible for the receiver of a message to ascertain its origin;
- Integrity: It makes it possible for the receiver of a message to establish whether a data message has been modified whilst in transit;

[25] http://www.rsasecurity.com/rsalavs/node.asp?id=2157 (accessed 01/04/06)
[26] http://www.webopedia.com/TERM/S/SSL.html (accessed 08/04/06)

- Non-repudiation: The sender of a data message cannot easily deny the fact that he or she sent the message or the contents thereof;
- Confidentiality: By using the encryption technology it is possible to ensure that only the intended recipient thereof can read it.

The term "*electronic signature*" extends to more than the functional equivalent of a handwritten signature on a paper document. An "*electronic signature*" not only identifies the person who communicated the information but also the contents of the data message. This added dimension will be of great benefit to parties transacting with each other through electronic medium as it will ensure greater certainty where paper documentation and handwritten signatures have in the past given rise to many disputes.

S 13 of the Act introduces two types of digital signatures into South African Law. It refers firstly to advanced electronic signatures. An advanced electronic signature is issued by an independent and trusted third party entity which must be credited by the authorities. The benefit of an advanced electronic signature is that it has a stronger evidential value than a "*normal*" electronic signature. S 13(4) states that "*an advanced electronic signature will be regarded as being valid, unless the contrary is proved. A party wishing to dispute the validity thereof will therefore bear the onus to prove invalidity.*"

The second or "*normal*" type of electronic signature, referred to above, is defined in the Act as "*data attached to, incorporated in, or logically associated with other data …. which is intended by the user to serve as a signature*". It was pointed out above that "*data*" means electronic representations of information in any form. A normal electronic signature can therefore be anything ranging from a sender of an electronic message's name that appears at the end of the message to a voice recording in which the author identifies himself by stating his name.

Parties to an agreement may choose which form of electronic signature they require for the conclusion of the contract. It is not necessary for parties to require the use

of an electronic signature at all as a valid agreement can still be concluded as long as their "*expression of intent*" can be established by the data message.[27]

Electronic signatures however also have certain disadvantages. Because it involves complex mathematical processes, users may struggle to understand the nature and application thereof. It requires certification and a third party verification regime which leads to an inevitable cost implication. The opinion has also been expressed that digital signatures are "*best suited for short-term contracts or documents which don't requirement extensive archiving, such as purchase orders electronic funds transfers and contracts for access to online services*".[28]

It is submitted that the levels of confidentiality and security currently provided by SSL protocols[29], adequately caters for the requirements of long-term assurers wishing to sell their products online. Our law does not require that a long-term insurance contract, or any document relating thereto, have to be signed by any of the parties thereto.

Retention of documents and evidential weight

The requirements laid down in the Financial Intelligence Centre Act in respect of obtaining and retaining a copy of the client's identity document, have been discussed above. Although FICA does not require the original identity document to be retained, it does require the copy of the identity document to be retained. In terms of s 14 of the Act such copy can be retained in electronic form. Reference was also made above to various provisions contained in the Financial Advisory and Intermediary Services Act that requires the retention of records evidencing disclosures made to the prospective policyholder, disclosures made by the policyholder to the assurer and record of advice

[27] Sec 13(5)
[28] Barnett P, *The Write Stuff? Recent developments in electronic signatures,* New South Wales Society for Computers and the Law, Journal : December 2001, Issue 46
[29] Discussed at page 34.

given prior to conclusion of the contract. By virtue of secs 11, 14 and 15 of the Act, assurers can now store vast numbers of documentation in electronic form at a significant savings in costs.

It is interesting to note that s 14 makes provision for possible changes that could be effected to a document as a result of transferring it into electronic form. This is a clear reference to the application of software that transforms a written document consisting of words into an electronic word document. The last mentioned word document in its electronic form might be different from the original document in various aspects, such as visual appearance and font size, although the contents remain virtually the same and is capable of manipulation.

S 15 of the Act deals with the admissibility and evidential weight of data messages. The section was enacted in light of the difficulties brought about by the previous Computer Evidence Act No. 57, of 1983 that has now been repealed by the ECT Act. Litigants wishing to rely on evidence which was in electronic format had to satisfy stringent requirements laid out in the Computer Evidence Act. It required qualified persons to authenticate computer printouts representing the evidence. This was often extremely difficult or impractical to the extent that parties to litigation found it extremely difficult to rely on electronic evidence.

S 15 of the Act now simplifies the production of evidence of data messages by effectively stating that it is admissible as evidence and that it must be given "*due evidential weight*". The section sets out the practise that a court must consider in assessing such "*due evidential weight*". This includes the following:-

> "*(a) The reliability of the manner in which the data message was generated, stored or communicated;*
> *(b) The reliability of the manner in which the integrity of the data message was maintained;*
> *(c) The manner in which its originator was identified; and*
> *(d) Any other relevant factor."*

S 15(4) will be of great relief and assistance to parties wishing to rely on evidence of data messages in a court of law. It states that a printout of such data message is admissible in evidence by its mere production in court. It furthermore states that upon being certified to be correct by "*an officer in the service of*" the party tendering the evidence, it will be "*rebuttable proof*" of the facts contained in the copy. Where the correctness of the contents of the copy or printout is therefore disputed, the onus will rest on the party disputing the correctness. As in the case of s 11 mentioned above, this provision will be of great benefit to assurers wishing to enter into online transactions in respect of its products on a large scale. The management personnel of long-term assurers will however be well advised to implement and follow programmes aimed at ensuring and documenting the integrity of the generation, storage and transmission of data messages and any documentation stored in electronic format. Such programmes must be able to give adequate particulars of all procedures implemented in the event of the integrity of evidence being questioned. The proper documentation of processes could be of tremendous assistance where key personnel, especially in the Information Technology field, might not be employed by the specific company anymore. Personnel in this field of expertise often provide their services on a consultancy basis as opposed to full-time employment at a specific company. This may prove to be problematic.

As stated above, most if not all the legislation applicable to long-term insurance transactions require the retention of documentation relating to transactions or the interaction between a long-term assurer and client. It was already mentioned that the ECT Act enables such information to be retained in electronic form. S 16 of the Act deals expressly with the retention of information and states that "*where a law requires information to be retained, that requirement is met by retaining such information in the form of a data message*". As is the case in ss 11 and 12 it requires that the information must be "*accessible so as to be usable for subsequent reference*" and the holder of the

information must be able to demonstrate that the data message accurately represents the retained information.

S 16(1)(c) requires furthermore that the "*origin and destination"* as well as the date and time that it was sent or received, must be able to be shown. Similar requirements are contained in s 17 which deals with the production of a document or information as opposed to the mere retention thereof. It similarly requires the producer of a document or information to be able to show that the integrity of the information has been maintained. The remarks made above in respect of the procedures and information systems put in place by the assurer are equally applicable to these two sections.

Automated Transactions

S 20 of the Act deals with the formation of an agreement by means of "*automated transactions*". An *"automated transaction"* is defined by the Act as *"an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct or data messages of one or both parties are not reviewed by a natural person in the ordinary course of such natural person's business or employment"*. S 20(a) confirms that an agreement may be formed *"where an electronic agent performs an action required by law for agreement formation"*. An "*electronic agent"* is defined by the Act as *"a computer program or an electronic or other automated means used independently to initiate an action or respond to data messages or performances in whole or in part, in an automated transaction"*.

The above is a clear reference to the growing trend in e-commerce of using computer programs or software to *"act on behalf of"* a party to an electronic transaction. An example of the application and utilisation of such software would be the computer program used by a company such as Kalahari.net in South Africa that offers *inter alia* books for sale over the Internet. It invites any person to purchase books online whereafter the books are delivered by post or courier to the purchaser. When the

purchaser concludes the transaction over the Internet on Kalahari.net's website, he or she in fact interacts not with a natural person in the employ of the Kalahari.net company, but rather with a computer program designed and programmed to interact with the purchaser on behalf of Kalahari.net. The conduct and data messages of the computer program employed by Kalahari.net is, for purposes of the transaction, not reviewed or controlled by a natural person in the employ of Kalahari.net. The software or computer program used by Kalahari.net for this purpose, therefore acts as *"electronic agent"* on its behalf and binds Kalahari.net to a valid agreement of sale without any natural person in its employ reaching consensus with the purchaser on behalf of the company.

Although the term *"electronic agent"* is used to give legal effect to the *"actions"* of the computer program, certain legal commentators point out that a computer program cannot be regarded as an *"agent"* in the legal sense of the word. Although in our law an agent acts in terms of a mandate received from his or her principal, such agent is still capable of forming and expressing intent for purposes of reaching consensus.

Prof. Christie in his work on the *"Law of Contract in South Africa"*[30] however reminds the reader that agreements can also be concluded tacitly. An offer can be made tacitly or accepted tacitly. If an offer is accepted tacitly it gives rise to a tacit contract or an implied contract. It can also be referred to as a contract by conduct. There is therefore in law no reason why it cannot be said that Kalahari.net in the example above, did not, through the conduct of the computer program, bind itself tacitly to a contract. By inviting a client to make an offer for the purchase of a book and by programming the computer to confirm to the purchaser that an agreement has been concluded and that the book will be delivered, Kalahari.net tacitly accepted the purchaser's offer.

In an article entitled *"Electronic Agents and the Formation of Contracts"* [31] Emily M Weitzenboeck refers to the difference of approach to the formation of a contract in civil law and common-law jurisdictions. Following the emphasise on liberalism in the

[30] Christie R H, *The Law of Contract*, 4th Edition, Butterworths, 2001, page 92
[31] Weitzenboeck E M, *International Journal of Law and IT,* September 2001, Oxford University Press

19th century in France, strong emphasize is placed in civil law jurisdictions on the "autonomy of the will" or the "supremacy of the inner will". In terms of this approach, also referred to as the subjective theory of consent, a court considering a dispute relating to the formation of agreements will examine the subjective intention of parties to an agreement. According to the common-law, however, a party is considered bound to an agreement when his behaviour or actions indicate that he bound himself. This is the so-called objective approach. She points out that English and American Law adopted the objective test of agreement. She also points out that one would run into difficulties if one tried to apply the subjective approach to a contract where at least one of the parties made use of an intelligent agent, as it is not possible to look at the *'inner psychological state of mind"* of an electronic agent. The objective test therefore suits the use of electronic agents better.

In applying the objective test, a court giving consideration to the formation of an agreement "*would apply the test of how a reasonable man in the shoes of the other contracting party would have interpreted the contractual statements made by the electronic agent, to see if they amounted either to a firm offer or an acceptance (depending on whether the offer was made by the agent or by the other party)"*. In such a case the actual internal workings of the electronic agent are not relevant.

In the same article, Weitzenboeck refers also to a model known as the Consumer Buying Behaviour (CBB) Model which was devised by Maes, Guttman and Moukas, members of the Software Agents Group at MIT Media Laboratory. The model identified six fundamental stages in the buying process which are (1) need identification, (2) product brokering, (3) merchant brokering, (4) negotiation, (5) purchase and delivery, and (6) product service and evaluation. She points out that the study conducted by the Software Agents Group found that the "*personalised, continuously-running and autonomous characteristics of agents"* make them well suited for mediating consumer behaviour relating to information filtering and retrieval, personalised evaluations, complex co-ordination and time placed interactions. It is therefore an ideal tool for purposes of the first stage referred to, being *need identification*. Long-term assurers

wishing to employ electronic agents to facilitate or mediate transactions for their products which could involve the rendering of financial advice, will be heartened by this observation.

Weitzenboeck also states the following, in summary:-

> *"Agents will no doubt be employed to assist human interaction through the various stages of a transaction from product and merchant brokering through to negotiation, sale, distribution and payment. It is not unreasonable to predict that, in time, agent technology will become sufficiently sophisticated to perform many if not all of these sorts of tasks without human oversight or intervention"*[32]

As stated, s 20(a) confirms that an agreement may be formed through an electronic agent. It states that such agreement may be formed where all parties to a transaction or either one of them uses an electronic agent.

In terms of s 20(d) a party interacting with an electronic agent will not be held to the agreement unless he or she was afforded the opportunity of reviewing the terms of the agreement *"prior to agreement formation"*. Any computer program or software implemented by a long-term assurer must therefore provide an opportunity to the prospective client to review the terms of the agreement before the contract is actually concluded. An agreement is also not valid where a person who interacted with an electronic agent made a material error during such interaction. To rely on the invalidity of an agreement in case of material error, the party relying on such invalidity will have to prove the following[33]:-

> *"(a) The electronic agent did not provide that person with an opportunity to prevent or correct the error;*
> *(b) that person notifies the other person of the error as soon as practicable after that person has learned of it;*

[32] Weitzenboeck *op cit* page 11
[33] Sec 20(e)

(c) that person takes reasonable steps, including steps that conform to the other person's instructions to return any performance received, or, if instructed to do so, to destroy that performance; and

(d) that person has not used or received any material benefit or value from any performance received from the other person"

In the case of an automated transaction relating to a long-term insurance product a person wishing to escape liability on the ground that he or she had made a material error will therefore have to show that the website did not provide him or her with an opportunity to correct the error and that he or she had notified the assurer of the error as soon as practicable after becoming aware of it.

The fact that s 20(e)(iv) also includes reference to the receipt of any material benefit or value can in the case of a long-term insurance policy be compared to receipt of any policy benefits. It is to be seen whether the fact that a person enjoyed death or disability cover for a period will in itself be regarded as *"any material benefit or value from any performance received from ….."* the assurer. It is submitted that the mere enjoyment of cover as opposed to receipt of the payment of benefits will not constitute material benefit or value for purposes of s 20(e)(iv).

It is important to note that s 20(c) creates a presumption that a party will be bound to the terms of an agreement where it utilised an electronic agent to form the agreement. Such presumption exists whether the company reviewed the actions of its electronic agent or the terms of the agreement, or not.

Communication of data messages and time and place of contracting

Part II of Chapter 3 of the Act contains provisions relating to the communication of data messages and therefore, by implication, to online contracting. It contains provisions relating to the time when and place where an agreement is concluded;[34] the time when a

[34] Sec 22(2)

data message is regarded as having been sent by the originator;[35] the time and place that a data message is regarded as having been received by the addressee [36] and the attribution of a data message to the originator.[37] The provisions contained in Part II of Chapter 3 are not obligatory and the parties to an electronic transaction are therefore free to agree on a different arrangement in respect of the above issues.

In terms of s 22(2) an agreement concluded between parties by means of the exchange of data messages is concluded *"at the time when and place where the acceptance of the offer was received by the offeror"*. As the section is not obligatory, a life assurer can insist that agreements concluded online be regarded as having been concluded at the place of business of the assurer. The obvious benefit to the assurer of such an agreement is the fact that disputes arising from the agreement would in all probability then fall within the jurisdictional area of the assurer.

It could be advisable for long-term assurers to insist on such an arrangement as it would not always be able to argue that (a) it had extended an offer to the prospective client which was open for acceptance and (b) that the agreement was therefore concluded when it received the data message containing the client's acceptance. In most instances a person applying for a long-term insurance policy completes an application form made available by the assurer. The information contained in the application form is then generally regarded as constituting an offer extended by the applicant for acceptance by the assurer. Often, as a result of its underwriting requirements, an assurer might decide to impose a health exclusion or a loading on the premium to be paid by the insured and it is then generally accepted that such loading or exclusion constitutes a counter-offer made by the assurer to the prospective client. It is then for the prospective client to consider and accept if he or she so wishes to accept the counter-offer of the assurer. It is therefore clear that, unless it is made clear by the assurer that contracts of insurance concluded by way of data messages will be regarded as having been concluded at the place of business of the assurer, policyholders declaring disputes with the assurer might in light of s 22(2)

[35] Sec 23(a)
[36] Sec 23(b)
[37] Sec 25

be able to argue that the contract of insurance was concluded in their own jurisdictional area.

S 23 creates three important presumptions. In the first instance a data message used for the conclusion or performance of an agreement will be regarded as having been sent by the originator when it enters an "*information system"* that is outside of the control of the originator. The term *"information system"* is defined in s 1 of the Act as *"a system for generating, sending, receiving, storing, displaying or otherwise processing data messages and includes the Internet*". *"Information system"* can therefore be a party's Internet services provider, a server used by a long-term assurer who receives and stores data messages, a mailbox on a personal computer of an individual person or even a fax machine. In all such cases the originator of the data message cannot retrieve it once it is sent to the information system of the addressee. Where the originator and the addressee share the same information system, a data message will be regarded as having been sent as soon as it is capable of being retrieved by the addressee. It is not clear to what extent an addressee's subjective inability to access his information system will be upheld as a defence to and deemed receipt in terms of s 23(a). Examples of subjective inability could be the fact that the addressee did not open his or her e-mails due to hardware or software failures or viruses. It is unlikely that the addressee would easily succeed with such a defence[38].

The second presumption created by s 23 is contained in s 23(b). A data message will be presumed to having been received by an addressee when it enters the information system of the addressee and is capable of being retrieved and processed by the addressee.

The third presumption relates to the originator as well as the addressee's usual place of business or residence. It will be presumed that data messages were sent from and received at the originator or addressees' usual places of business or residence. In a similar manner s 25 creates a rebuttable presumption that a data message was authored and transmitted by the originator where it was sent by him or her personally or a person

[38] Buys et al *op cit* page 98

acting on his or her behalf. The presumption also applies where a data message was sent by an information system that was programmed to act on behalf of the originator.

Reference was made above to the use of an electronic agent during the conclusion of an automated transaction and this section makes it clear that a message created by such electronic agent will be presumed to have been sent by the electronic agent. If a person or entity making use of such electronic agent wishes to escape the consequences of a data message sent incorrectly by its electronic agent, it would bear the onus to prove that the information system did not properly "*execute such programming*". It is submitted that a party wishing to escape liability in such a situation would in any event bear the onus to prove that the electronic agent malfunctioned and it was therefore strictly speaking not necessary for the legislator to enact a presumption in this regard.

CHAPTER IV

CONSUMER PROTECTION IN ONLINE TRANSACTIONS

In this Chapter, the various consumer protection measures contained in the ECT Act will be studied. Reference will also be made throughout to consumer protection provisions contained in other legislation that apply to the selling of long-term insurance products. The Chapter will also consider the recently published *Protection of Personal Information Bill* as it will have an important impact on the processing of personal information that will always form an integral part of online transactions.

Consumer protection under the ECT Act

Chapter VII of the ECT Act provides online consumers with a number of rights that will apply to online transactions, additional to the rights already referred to above in terms of the legislation applicable to the long-term insurance industry. In many instances the provisions correspond with the rights provided by the legislation referred to and long-term assurers offering their products online will have to ensure that they adhere to the minimum standards and requirements laid down in both sets of legislation. It must however be noted that s 44 which provides for the cooling-off period of seven days is not applicable to an electronic transaction for financial services, which in terms of s 42(2)(a) includes "*investment services, insurance and reinsurance operations, banking services and operations relating to dealings in securities*".

The rights afforded by the ECT Act can be summarised as follows:-

- The right to disclose information about the product supplier, it's goods, services and prices[39];
- The right to review a summary of an electronic transaction before deciding to proceed, amend or terminate a transaction[40];
- The right to a secure online payment system[41];
- The right to a cooling-off period of seven days[42];
- Rights relating to the receipt of spam communications[43]; and
- The right to performance within thirty days of a transaction.[44]

S 43 contains a list of 18 items of information that must be *"made available to consumers on the website"* where products are offered for sale. These are:-

> *"(a) Its full name and legal status;*
> *(b) its physical address and telephone number;*
> *(c) its web site address and e-mail address;*
> *(d) membership of any self-regulatory or accreditation bodies to which that supplier belongs or subscribes and the contact details of that body;"*

Long-term assurers will have to provide the contact details of the Life Offices Association (the LOA). They will also have to provide details of their accreditation with the Financial Services Board in terms of the FAIS Act, as well as the contact details of the FSB.

> *"(e) any code of conduct to which that supplier subscribes and how that code of conduct may be accessed electronically by the consumer;"*

[39] Sec 43(1)
[40] Sec 43(2)
[41] Sec 43(5)
[42] Sec 44
[43] Sec 45
[44] Sec 46

Reference must here be made to the various Codes of Conduct of the LOA and FAIS Codes of Conduct. The LOA's website address, where the Codes can be viewed, will have to be stated.

> *"(f) in the case of a legal person, its registration number, the names of its office bearers and its place of registration;*
> *(g) the physical address where that supplier will receive legal service of documents;*
> *(h) a sufficient description of the main characteristics of the goods or services offered by that supplier to enable a consumer to make an informed decision on the proposed electronic transaction;*
> *(i) the full price of the goods or services, including transport costs, taxes and any other fees or costs;"*

It was already pointed out above[45] that the FAIS Act requires full disclosure of detailed information about the product sold to a client. In the course of a normal (non-online) transaction, such information and disclosures are provided to the client in the form of the contents of marketing material, the application-form completed and signed by the client, the written quote provided to the client as well as the contract issued and delivered to the client. The General Code published in terms of the FAIS Act also requires that the information be "*provided timeously so as to afford the client reasonably sufficient time to make an informed decision about the proposed transaction*". Reference was made above to the various ways that the required disclosures can be made on a Long-term assurer's website.

The comments under (h) above are equally applicable to this requirement.

> *"(j) the manner of payment;"*

In the case of a Long-term insurance policy, "payment" will be in the form of premiums. It will always be important to stipulate the exact date upon which the first premium is to be paid. Often the cover in terms of a policy will not start until payment of

[45] Page 22

the first premium, or within a stipulated period eg. 30 days, prior to receipt of the first premium. Because of the possible dispute that can arise as to the meanings of "payment" and "receipt" in the modern electronic banking world, clear stipulations in this regard will be to the benefit of both the client and the assurer.

Reference can also be made here to the provisions contained in ss 43(5) and (6) that compels the seller to implement technology (a "*payment system*") that will ensure safe and efficient electronic payments. The seller can be held liable, in terms of the Act, for any damage suffered by the consumer that occurred as a result of the seller's failure to comply with the Act in this regard.

> "*(k) any terms of agreement, including any guarantees, that will apply to the transaction and how those terms may be accessed, stored and reproduced electronically by consumers;"*

A distinction must be made between the terms and conditions "normally" applicable to a certain long-term insurance contract (or the so-called "generic" terms) and the terms specifically applicable to each individual's contract. Each individual contract will be different in respect of the type of benefit it provides, the premium payable, the term of the contract and health exclusions and guarantees that might be applicable. The normal or "generic" terms applicable "in general" to a specific product or type of product can therefore be made available for perusal on the website of the assurer, but it will always be necessary to provide each individual client with the exact terms of his or her policy contract. It is submitted that there exists no reason why, instead of providing the client with a paper-based copy of the policy agreement, an electronic version thereof cannot be e-mailed to him or her.

> "*(l) the time within which the goods will be dispatched or delivered or with in which the services will be rendered;*

(m) the manner and period within which consumers can access and maintain a full record of the transaction;"

As stated above, each individual client will have to be provided with a copy of his or her policy contract. There is no reason why this cannot be done electronically.

"*(n) the return, exchange and refund policy of that supplier;*

(o) any alternative dispute resolution code to which that supplier subscribes and how the wording of that code may be accessed electronically by the consumer;"

Within the financial services industry alone, there are currently five different quasi-judicial statutory and voluntary adjudicative tribunals:

- The Ombud for banking services, a voluntary scheme;
- The short term insurance Ombud, a voluntary scheme;
- The long term insurance Ombud, a voluntary scheme;
- The pension funds adjudicator, empowered by Chapter VA of the Pension Funds Act 24 of 1956; and
- The Ombud for FSP's, empowered by Chapter VI, part I of the Financial Advisory and Intermediary Services Act 37 of 2002.

"*(p) the security procedures and privacy policy of that supplier in respect of payment, payment information and personal information;"*

The next Chapter will discuss the Data Protection and Privacy legislation soon to become law in South Africa. Long-term assurers will have to study the requirements of such legislation closely to ensure that their security procedures and privacy policies are fully compliant. The website will have to make such information available to the client.

> *"(q) where appropriate, the minimum duration of the agreement in the case of agreements for the supply of products or services to be performed on an ongoing basis or recurringly; and"*

Comments under (k) above are equally applicable to this requirement.

> "*(r) the rights of consumers in terms of s 44 where applicable*."

The cooling-off provisions contained in s 44 are not applicable to electronic transactions involving financial services. In terms of the requirements of the FAIS Act referred to above specific cooling-off periods will apply to transactions for long-term policies and must be disclosed to the client.

Additional to the information that must be provided on the web-site, the consumer must also be provided with the opportunity:-

> "*(a) to review the entire electronic transaction;*
>
> *(b) to correct any mistakes; and*
>
> *(c) to withdraw from the transaction, before finally placing any order."*[46]

Failure to comply with the provisions relating to the information that must be disclosed on the web-site or the opportunity to "*review*", "*correct*" and "*withdraw*" will provide the consumer with the right to cancel the transaction "*within fourteen days of receiving the goods and/or services*". It is noted that the Act does not render the transaction automatically invalid due to such failure, but merely grants the consumer the right to withdraw from it. It is therefore similar to a "*cooling-off*" provision. It is submitted that the date of "*receiving the goods or services*" will be the date upon which the policyholder received the policy document, whether in paper or electronic form. Reference was made above to the cooling-off period of thirty days contained in Part IV of

[46] Sections 43(2)(a) – (c)

the Policyholder Protection Rules published in terms of the Long-term Insurance Act.[47] The Policyholder Protection Rules refer to *"a period of thirty days of receipt of the summary contemplated in Section 48 of the (Long-term Insurance) Act"*.

A *"cooling-off period"* or right afforded to a consumer is, it is submitted, a right to review a purchase or transaction within a time period and then to cancel the purchase if so elected. The consumer is granted this opportunity to reconsider a purchase normally where he or she might have been influenced to enter into the transaction as a result of compelling and enticing marketing material. The consumer can fully review a transaction upon receipt of the product or terms of the transaction and should then, it is submitted, exercise the right of withdrawal within a specified period of receiving the product or terms. It is therefore submitted that the words *"within fourteen days of receiving the goods or services under the transaction"* as it appears in s 43(3) were intended by the legislature to mean, *in the case of a transaction for a long-term insurance policy* to be the date upon which the consumer received the policy document.

The policyholder enjoys in any event, in terms of the Policyholder Protection Rules, a cooling-off right that extends to thirty days of receiving the policy document or summary thereof.

Protection of Personal Information

Any transaction for the issuing of a long-term insurance policy, will by the nature of the transaction and product, involve the obtaining of confidential personal information of the consumer. To enable the assurer to properly underwrite the applicant, i.e. assess the risk profile of the applicant and thereby determine an appropriate premium to be paid, personal information such as the following must be obtained from the applicant:-

(a) Medical information, including current and historical facts;

[47] Page 14

(b) Professional and lifestyle (sporting or risky activities);

(c) Income, smoking and drinking habits.

Apart from the highly personal nature of the above information, an applicant will also be required to disclose information such as his or name, gender, race,[48] address, marriage status, bank account details and insurance portfolio.[49] Chapter VIII of the ECT Act deals with the protection of personal information. The Act defines personal information *inter alia* as *" information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social original, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the individual"* .

The definition contains numerous other items of information about an individual as *"personal information"* and is clearly intended to give a broad definition of the term. This approach of giving a broad definition of personal information is also found in the Promotion of Access to Information Act, No. 2 of 2000, which was promulgated to provide individuals with a procedure by which to enforce their constitutional right of access to information against government bodies as well as private bodies holding records of such an individual. Although the last mentioned Act was promulgated to provide the right of access, it also contains provisions that relate to the protection of personal information. As stated, it contains a similarly wide definition of *"personal information"*.

Chapter VIII of the Act endeavours to provide some protection to the privacy of personal information. It must be pointed out, however, that it applies only to personal information that was disclosed during the course of (*"through"*) an electronic transaction. It is a relatively short Chapter containing a list of *"principles for electronically collecting personal information"*. The principles reflect universally adopted data protection

[48] Financial Sector Charter, http://www.treasury.gov.za/press/other/2003101701.pdf
[49] In terms of the LOA Code on Good Practice for Disability Insurance, assurers must ensure that policyholders are not over-insured for purposes of disability benefits. Information must therefore be obtained of other policies which provides similar benefits.

principles as already adopted and implemented in foreign jurisdictions such as the European Union. Chapter VIII is not obligatory and it allows *"data controllers"* to voluntarily subscribe to the principles.

The fact that the Act therefore gives relatively little attention to the important issue of data privacy can probably be ascribed to the fact that the South African Law Commission is currently drafting legislation that will specifically apply to the issues of data protection and privacy. Although our constitution protects the right to privacy in s 14 thereof, no statute currently exists in South Africa that gives comprehensive protection and content to the right. The ECT Act and the Promotion of Access to Information Act merely gives a measure of protection.

During October 2005, the South African Law Reform Commission published Discussion Paper 109 (Project 124) entitled "*PRIVACY AND DATA PROTECTION"*. It included a Draft Bill and to *"Promote the protection of personal information processed by public and private bodies; to provide for the establishment of an Information Protection Commission, and to provide for matters incidental thereto"*. Interested parties were invited to provide comment on the Discussion Paper on the Draft Bill by 28 February 2006, which date was extended to 31 March 2006.

In the introduction to the Discussion Paper the following is stated in reference to electronic transactions:-

> *"Concern about information protection has increased worldwide since the 1960's as a result of the expansion of the use of electronic commerce and the electronic environment. The growth of centralised government and the rise of massive credit and insurance industries that manage vast computerised data bases have turned the modest records of an insular society into a bazaar of information available to nearly anyone at a price"*

and

> *"the question is no longer whether information can be obtained, but rather whether it should be obtained and, where it has been obtained, how it should be used. A fundamental assumption underlying the answer to these questions is that if the collection of personal information is allowed by law, the fairness, integrity and effectiveness of such collection and use should also be protected"*.

The Paper refers to the fact that legislation already exits in foreign jurisdictions dealing with the protection of personal information and it refers specifically to *"two crucial international instruments"* being:-

(a) the Council of the Europe's 1981 Convention for the Protection of Individuals with regard to the automatic processing of personal data (CoE Convention); and

(b) the 1981 Organisation for Economic Co-Operation and Developments (OECD) Guidelines governing the protection of privacy and trans border data flows of personal data.[50]

The Commission points out that these agreements had a big influence on legislation around the world dealing with data protection and privacy as they contain technologically neutral principles relating to the collection, retention and use of personal information.

It is necessary for purposes of this Paper to consider the Draft Provisions contained in the Bill as it will have an important and direct impact on all electronic transactions once it becomes law. The Bill essentially aims to protect the privacy of personal information by prohibiting the processing thereof in any manner that is not consistent with the conditions and principles set out in the Bill. Failure to comply with the Rules and Obligations contained in the Bill could result in the laying of a complaint to the Information Protection Commission to be instituted in terms of the Bill, or civil action.

[50] www.doj.gov.za/salrc/dpapers/ (accessed 01/04/06)

As in the case of the Promotion of Access to Information and ECT Acts, a broad definition is given to the term *"personal information"*. The definition is in fact almost similar to the definitions contained in the said legislation.

Chapter III of Bill contains the all important *"Conditions for the lawful processing of personal information"*. It contains in Part A of the Chapter a series of eight *"Information Protection Principles"* that must be adhered to during the processing of personal information. *"Processing"* is defined in the Bill as:-

> *"any operation or any set of operations concerning personal information, including in any case the collection, recording, organisation, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or making available in any form, merging, linking, as well as blocking, erasure or destruction of information"*.

There can be little doubt that any online transaction involving the sale of a long-term insurance policy will qualify in terms of this wide definition as the *"processing"* of personal information. Each of the principles will now be discussed briefly.

Principle 1: Lawfulness of Processing: In terms of this principle, personal information must be processed in accordance with the law and in a proper and careful manner so as not to intrude upon the privacy of an individual to an unreasonable extent. Personal information may only be obtained and processed for the purpose for which it was collected. In the case of long-term insurance transactions, this could mean that personal information must not be used by the assurer for any other purpose than the proper underwriting and issuing of a policy contract to the insured. The first principle does however allow for the processing of personal information where a data subject has given consent thereto. This concession is read to mean that a data subject can give his or her consent for the extended use of personal information such as for purposes of

marketing new of further products to the person, if such specific consent has been obtained from the person.

Reference can here be made to s 24 contained in Part B of Chapter III of the Bill which prohibits the processing of *"special personal information"* unless the data subject has given his or her explicit consent thereto. The section refers *"special personal information"* as information concerning a person's "*religion or philosophy of life, race, political persuasion, health or sexual life, or personal information containing Trade Union Membership, criminal behaviour, or unlawful or objectional conduct connected with a ban imposed with regard to such conduct"*. The fact that reference is made also to information about the *"health"* of a person can make the section specifically applicable to the long-term insurance business.

The first principle also states that personal information must be collected directly from the data subject unless it is contained in a public record or unless the person consents to the collection of such data from a third party source.

Principle 2: Purpose Specification: The terms of this principle personal information must be collected for "*a specific, explicitly defined and legitimate purpose"*. The data subject must be made aware of the purpose of the collection of the information and possible recipients thereof. The principle importantly also deals with the retention of records by stating that records of personal information must no be kept longer than is necessary for achieving the purpose for which it was collected, unless required in terms of other legislation. Records must be destroyed as reasonably practicable after this date. Insurance companies will in future have to ensure that they have processes in place to identify such *"defunct"* records and for it to be destroyed.

Principle 3: The Limitation on Further Processing: In terms of this principle personal information may not be further processed in a way that is not compatible with the purpose for which it was collected. The following can be taken into account for determining whether information may be further processed:-

"(a) The relationship between the purpose of the intended further processing and the purpose for which the information has been obtained;

(b) The nature of the information concerned;

(c) The consequences of the intended further processing for the data subject;

(d) The manner in which the information has been obtained; and

(e) Any contractual rights and obligations existing between the parties."

Principle 4: Quality of information to be ensured: In terms of this principle, steps must betaken to ensure that personal information collected for a specific person is complete, not misleading, up to date and accurate. It is submitted that this requirement could mean that long-term assurers must from time to time require the policyholder to confirm that information on record pertaining to that person is still correct. Processes will have to be put in place to allow for this requirement.

Principle 5: Openness: In terms of this principle information may only be collected if it has notified the Commission in terms of the Act. In terms of s 47 of the Bill, the processing of personal information must be *"notified to the Commission before the processing is started"*. Certain categories of processing which *"are unlikely to infringe the fundamental rights and freedoms of (a) data subject"* may be exempted from notification in terms of s 49. Creating the Office of the Information Protection Commission is intended to promote transparency, accountability and effective governance of those entities that obtain, process and store personal information. The duties of the Commission are set out in the Bill[51] and includes the promotion of public understanding and acceptance of information privacy and protection thereof, the monitoring of compliance, the provisions of the Bill, consultation with members of the public and other role players, the investigations of complaints about alleged violations of

[51] Sec 39(1) of the Bill

the principle, research and reporting and the issuing of Codes of Conduct dealing with the objectives of the Bill.

Principle 6: Security Safeguards: In terms of this principle, entities collecting and processing personal information must implement procedures to secure the integrity of personal information which will safeguard it against *"the risk of loss of, or damage to or destruction of personal information and against the unauthorised or unlawful access to or processing of (it)"*. Security compromises must be notified to the Commission.

Principle 7: Individual Participation: The provisions contained under this principle are similar to the rights of access to information provided for in the Promotion of Access to Information Act. It gives a data subject the right of access to personal information held by an entity relating to the subject. It furthermore allows the subject to insist on the correction of personal information where required. It is submitted that long-term assurers should provide a policyholder with online access to all information held by an assurer in respect of that person so that the accuracy thereof can be reviewed by the policyholder at any relevant time.

Long-term assurers should bear in mind that they could be holding information about a person to which he or she should not be given unqualified access. Reference must be made here to Sec. 61 of the Promotion of Access to Information Act, that provides for the limiting of access to *" a record provided by a health practitioner … about the physical or mental health, or well-being"* of an individual. Access to such records should not be granted freely if the grantor is of the opinion that the disclosure of the record to the relevant person "*might cause serious harm to his or her physical or mental health, or well-being*". Adequate provision must first be made for "*such counselling or arrangements as are reasonably practicable before, during or after the disclosure of the record to limit, alleviate or avoid such harm to the relevant person*". As applying for life insurance could mean the undergoing of HIV-testing, life assurers could receive information about an applicant's health that should best be disclosed to him or her by a

health practitioner and in a manner that will not cause undue emotional or physical hardship.

A similar *caveat* does not appear in the Bill and the legislator should give consideration to the inclusion thereof. Life assurers should also ensure that unqualified access is not granted to all categories of information as the disclosure thereof to a person could be detrimental to such persons health or wellbeing in certain, albeit exceptional cases.

Principle 8: Accountability: This principle places the duty on processors of personal data to ensure that it has implemented measures to give effect to the principles set out in the Bill.

The Bill furthermore requires each entity which will process personal information to appoint an *"Information Protection Officer"*. It will be this person's duty to ensure that the entity processes information in compliance with the Bill and to deal with requests for access to personal information by data subjects. The role of such Information Protection Officer will not be dissimilar to the Information Officer required in terms of the Promotion of Access to Information Act. The Information Protection Officer will also be tasked with liaising with the Information Protection Commission in relation to the investigations that the Commission must carry out in terms of Chapter VI of the Bill. One of the duties of the Commission will be to investigate any processing which will involve information relating to criminal or unlawful conduct of third parties, processing of information for purposes of credit reporting and processing of special personal information referred to above. The Information Protection Officer will have to notify the Commission where any of the above is to occur whereupon the Commission may investigate the processing procedure.

This reporting duty can be compared to the duties placed on a Money Laundering Officer in terms of the FICA Act. In the case of the FICA Act, the object of the Act and therefore the reason for the reporting duty is the combating of criminal activity in the

form of money laundering. In the case of the Protection of Personal Information Bill the object is different, being the eradication of practices which infringes on the constitutional right to privacy of individuals.

These two Acts illustrate to an extent the conflict and tension that exists between the promotion and protection of individual privacy on the one hand, and the necessity for crime prevention authorities to gain access to information in the commercial arena in order to combat crime effectively. The growing body of business that is conducted through the electronic medium (through electronic transactions) and therefore the growing body of information about the people and money involved therein, makes it increasingly necessary for law enforcement agencies to have access to the records and perhaps even the communications generated thereby.

The Regulation of Interception of Communications and Provision of Communication-related Information Act

The Regulation of Interception of Communications and Provision of Communication-related Information Act, No. 70 of 2002, (the "RIC Act") was promulgated to regulate the interception of "*certain communications"*. Although this Act prohibits the interception of communications as a general rule, it contains various provisions which allows for the interception or monitoring of communications. Any business entity, including Long-term assurers, that intends conducting its business through the electronic medium will have to give careful consideration to the provisions of this Act. Of particular concern is the requirement that "telecommunication service providers", which by definition in the Act includes "internet service providers", must "*provide a telecommunication service which has the capability to be intercepted*".[52] The definitions of "telecommunication service provider", "telecommunication service" and "telecommunication system" are fairly broad and could arguably include the offering of products for sale through a website. The definition of "internet service provider"

[52] Sec 30

strengthens this concern. It defines the term as "*any person who provides access to, or any other service related to, the Internet to another person, whether or not such access or service is provided under and in accordance with a telecommunication service licence issued to the first-mentioned person under Chapter V of the Telecommunications Act*". This could oblige an entity with such websites to ensure that it utilises technology and information systems that "*has the capability to be intercepted*". A further concern is the fact that a "decryption key holder" can in certain circumstances be forced to hand over the decryption key. Admittedly an "interception direction" or a "decryption direction" which is akin to a search warrant must first be issued by a "designated judge", but it could lead to abuse by law enforcement agencies and an erosion of individuals' rights of privacy. Search warrants are usually granted on an *ex parte* basis and the subject, whose privacy is about to be infringed does not have the opportunity to show that the invasion is not justified. It is to be seen how judges (in chambers) and our courts will deal with these issues. It is also to be seen whether this interference with the e-commerce processes will cause it unnecessary harm or inhibit its growth and success.

CHAPTER V

LIABILITY: NON-COMPLIANCE WITH STATUTORY PROVISIONS, AND CONTRACTUAL AND DELICTUAL LIABILITY

It is clear that the long-term insurance industry is a highly regulated industry and long-term assurers must therefore be constantly mindful of the risks that it could incur if it fails to comply with the various statutory requirements imposed on it. The aim of this Chapter is to consider the implications of non-compliance with the various regulatory and statutory requirements which includes statutes such as the ECT Act, the RIC Act and Protection of Personal Information Bill that is expected to become law in the near future. This Chapter will also deal with the possible contractual and delictual liability that could flow from actions or omissions that may occur during electronic transactions for long-term insurance products.

Long-term Insurance Act, 52 of 1998

Part VIII of the Long-term Insurance Act deals with offences and penalties. In terms of s 67(a), a long-term assurer which contravenes certain requirements contained in the Act shall be guilty of an offence and liable on conviction to a fine not exceeding R100000.00. These requirements relate *inter alia* to:-

(a) ……..;

(b) The publishing of any misleading communication, brochure or advertisement that relates to the business of a long-term assurer or where such publication is misleading or contrary to the public interest or contains an incorrect statement of fact where any such advertisement, brochure or communication fails to include the name of the long-term assurer underwriting a long-term policy, and where an offence is also committed.

(c) The application to a person's business, without approval of the Registrar, of the name or description such as "*insure*", "*assure*" or "*underwrite*" or any derivative thereof unless he or she is a long-term assurer.

(d) The carrying on of the business of a long-term assurer without being authorised to do so.

(e) The granting of a free choice to clients when a new policy or existing policy is to be made available for purposes of securing debt (s 44 of the Act).

(f) The provision of any valuable consideration as an inducement to enter into, continue, vary or cancel a long-term policy, the provision to the client of a summary of the policy agreement (s 48 of the Act).

(g) The requirements and limitations set out in the regulations pertaining to the provision of policy benefits, the surrender of policy benefits and the making of a loan upon security thereof (s 54 of the Act).

(h) The limitations on benefits to be provided in the event of the death of an unborn or of certain minors (s 55 of the Act).

(i) The rules relating to the protection of policyholders in terms of s 62 of the Act.

A fine not exceeding R1m can be imposed in case of the carrying on of the business of a long-term assurer without being authorised to do so (s 15 of the Act).

The Financial Advisory and Intermediary Services Act 37 of 2002

In terms of s 10 of the Act the authorisation of a financial services provider may be withdrawn by the Registrar where it has *"contravened or failed to comply with any provision of (the) Act in a material manner"*. In terms of s 17 authorised financial services providers must appoint compliance officers to monitor compliance with the Act. They must also submit reports to the Registrar in a manner prescribed by the Registrar and at such times as prescribed in terms of Chapter VI of the Act. The Office of the Ombudsman for Financial Services Providers was created by Chapter VI. The Ombud

has the power to award compensation where a client who lodged a complaint with the Ombud has suffered financial prejudice or damage. It may also issue a direction to the authorised financial services provider guilty of causing prejudice or damage or take such steps in relation to the complaint as the Ombud deems appropriate and just.

The Ombud may make any order which a court may make[53]. Part II of Chapter VII provides the Registrar with the power to institute civil action against any person contravening any provisions of the Act and may also institute action in a court for damages flowing from any non-compliance[54]. The Registrar may also declare certain business practices "*undesirable*"[55] the authorised financial services provider concerned may thereafter not carry on the business practice concerned.

A fine of an amount of not exceeding R1m or imprisonment for a period not exceeding 10 years may be imposed upon any person who contravenes such order relating to an undesirable practice or:-

(j) if it acts as financial services provider without authorisation (s 7);
(ii) fails to maintain records for the prescribed minimum period of 5 years (s 18).

Financial Intelligence Centre Act 2 of 2000

Chapter IV of the Act creates a long list of offences which includes *inter alia*, the failure to identify persons, the failure to keep records, the destruction or tampering with records and the failure to report electronic transfers (ss 46 to 66). It is also an offence to fail to give effect to a "*monitoring order*" issued by a judge in terms of s 35 of the Act. An order will be granted in terms of this section where there are reasonable grounds to suspect that a person is transferring or has transferred the proceeds of unlawful activities or property which is connected to an offence. In terms of s 68 of the Act a penalty of

[53] Sec 28
[54] Sec 33
[55] Sec 34

R10m or imprisonment of a period not exceeding 15 years may be imposed if a person is convicted of an offence mentioned in the Chapter. The lesser fine of R1m or imprisonment for a period not exceeding 5 years may be imposed in cases of contravention of ss 55, 61 and 62 which deals with a failure to send a report to the Financial Intelligence Centre, a failure to formulate and implement internal rules to ensure compliance with the Act; and failure to provide training to staff or appoint a compliance officer.

Electronic Communications and Transactions Act 25 of 2002

In terms of Chapter VII that deals with consumer protection, in the cases of any non-compliance with the provisions of the Chapter may be referred to the Consumer Affairs Committee (s 49). It was pointed out above that compliance with Chapter VIII that deals with the protection of personal information is voluntary and the Act therefore contains no offences or penalties in this respect. Chapter XII of the Act deals with the appointment of so-called "*cyber inspectors*". At date hereof no such inspectors have been appointed and it is still to be seen whether any such inspector will be appointed in the foreseeable future. In terms of s 81 of the Act these inspectors will have the power to monitor and inspect any web-site or activity on any information system in the public domain and to report any unlawful activity to the appropriate authority. It is furthermore stated that any statutory body, including the South African Police Service, vested with powers of inspection or search any seizures in terms of any law may be assisted by the cyber inspectors during an investigation. Chapter XIII of the Act declares it a criminal offence to obtain unauthorised access to, interception or interference with a data message. It also deals with several other forms of so-called "*cyber crime*" including computer-related extortion, fraud, forgery, attempt and aiding and abating. In terms of s 89 of the Act a person guilty of contravening several provisions contained in the Act is liable to a fine (not stipulated) or imprisonment for a period not exceeding 12 months. These offences relate to:-

(i) The accreditation of authentication products and services;

(ii) The accreditation by the Minister of Foreign Products and Services (s 40) or the requirements in terms of critical data basis administrators in terms of Chapter VIV of the Act;

(iii) The hindering or obstructing of a cyber inspector (s 80);

(iv) Unauthorised access to computer inception or interference of data in terms of s 86 of the Act.

The Protection of Personal Information Bill

The Proposed Bill provides for the institution on civil action by the Commission (or in this case the data subject) against any party who has contravened or not complied with any provision in the Act. In terms of this section a claim may be instituted for an amount to be determined by the court as compensation for patrimonial and non-patrimonial damages suffered by the data subject in consequences of a contravention. The amount of damages is limited to an amount not exceeding three times the amount of any profits or gain which may have accrued to the person involved as a result of the act or omission. Chapter VI of the Bill deals with offences and penalties. S 91 specifically deals with penal sanctions in case of an offence in terms of the Act. In case of a contravention of s 88 (obstructing of the work of the Commission) a fine (unstipulated) or imprisonment for a period not exceeding ten years be imposed. In any other case a fine (unstipulated) or imprisonment for a period not exceeding twelve months may be imposed.

Contractual and delictual liability

Apart from the risks and liability that may be incurred as a result of non-compliance with legislation, long-term assurers offering the sale of their products through the electronic medium must bear in mind the normal principles of contractual and delictual liability that will apply to their business. As they take part in commercial transactions numerous acts and omissions could give rise to claims for damages. Websites could contain erroneous

information about products which could induce purchasers to enter into transactions that they would otherwise have desisted from. Financial calculators made available on a website to illustrate future benefits could contain errors. Information provided or elections made by the purchaser, such as the particulars of a bank account from which premiums will be paid or the nomination of a beneficiary on a long-term policy or the disclosure of material information, could be recorded or processed incorrectly. Important contractual terms, such as the amount of death cover that the policyholder will enjoy in terms of the contract, could be stated incorrectly due to a systems error. Personal information of a policyholder could inadvertently be disclosed to a third party, causing the policyholder embarrassment and emotional distress.

In all such cases, policyholders could claim that they suffered damages as a result of the act or omission and could hold the insurance company liable for their loss. It is therefore important to consider the principles that would apply when such claims for damages are instituted.

A distinction must firstly be made between patrimonial loss and non-patrimonial loss. Patrimonial loss can be defined as *"the loss or reduction in value of a positive asset in someone's patrimony or the creation or increase of a negative element of his patrimony (a patrimonial debt)"*.[56] Non-patrimonial loss refers to the injury to personality and can be defined as *"the diminution, as a result of a damage-causing event, in the quality of the highly personal (personality) interests of an individual in satisfying his legally recognised needs, but which does not affect his patrimony"*.[57]

In South African Law, actions for the recovery of patrimonial loss can be brought as actions based in contract (if a contractual relationship exists between the parties) or in delict. Where the action is brought in delict it is based on the *lex aquilia*. An action for non-patrimonial loss is brought by way of an *actio iniuriarum*[58].

[56] Visser P J and Potgieter J M, *Law of Damages,* Juta and Company Limited, 1993, Page 42
[57] Visser P J and Potgieter J M *op cit* page 85
[58] Boberg PQR, *The Law of Delict,* Juta and Company Ltd, 1984, Volume 1, page 18

There are various ways that long-term assurers conducting business as aforesaid could expose themselves to claims for damages. As stated, transactions for long-term products are based in contract. As can be expected, disputes can easily arise as to the terms applicable to a specific contract, the interpretation of the terms thereof, the obligations created thereby, or the validity of claims.

A party claiming damages due to a breach of contract will be entitled to insist that that he be placed in the position that he would have been had the contract been properly performed. This is referred to as *"positive interesse"* which can also be defined as the total interest which a contracting party has in the other party fulfilling his contractual obligations.[59] The party claiming damages will furthermore have to prove a causal link between the breach of contract and the alleged damages. Our courts will also limit the extent of the damages to be recovered by requiring that the damages *'flow naturally and generally from the kind of breach of contract in question"* or that *"in the special circumstances of the case existing at the conclusion of the contract, the damages were within the contemplation of the parties …. and that the contract was entered into on the basis of such knowledge"*[60]

In his book entitled *Computer Law*[61], Colin Tapper points out that a distinction should be made between business and consumer transactions. He states that, in the case of business transactions, the law is prepared to *"stand back and to let the parties reach the agreement which they themselves consider best meets their needs"*. In the case of consumer transactions however, the law is more interventionist *"because it recognises frequent inequality of knowledge, means, and acumen which prompts it to offer a minimum safety net of protection to the consumer"*. Although Tapper makes this statement with reference to English Law it might well be or become equally relevant to South African Law. The growing emphasise that is placed in South Africa on consumer protection as seen in this paper will in all probability have an influence on the way our

[59] Visser P J and Potgieter J M *op cit* page 20
[60] Harms L T C, *Amlers Precedents of Pleadings*, Butterworths, 4th Edition, 1993, page 102
[61] Tapper C, *Computer Law* , Longman Group UK Ltd, 4th Edition, 1998, page 140

courts view questions relating to contracting, breach of contract and damages flowing therefrom.

The second and very important basis upon which liability for damages can be incurred is delict. This refers to the damages that a party can claim from another due to the wrongful act or omission of that party. In our law such damages can be recovered by way of the *actio lexis aquiliae* which entitles a plaintiff to recover patrimonial loss (which can include a purely economic loss) which the plaintiff suffered as a result of a wrongful and negligent act of a defendant.[62] The wrongfulness can be constituted either as the breach of a common-law right or the breach of a statutory duty or the breach of a duty of care. As in the case of a claim for damages due to a breach of contract, a plaintiff must prove a causal link between the wrongful action and the damages suffered. As in the case of contractual damages, the plaintiff must also convince the court that the alleged damages claimed are not too remote from the action or event that caused it or that it were not foreseeable. Where the wrongfulness is based on a breach of a duty of care (i.e. negligence) the plaintiff must prove that a *diligens paterfamilias* in the position of the defendant would have foreseen the reasonable possibility of his conduct causing injury to the other person or that person's property; that such *diligens paterfamilias* would have taken reasonable steps to guard against such occurrence and that the defendant had failed to take such steps. This is generally accepted as the test for negligence in our law.[63]

In the context of electronic transactions within the long-term insurance business, damages caused by a wrongful act or omission will normally give rise to financial or "pure economic loss". Pure economic loss usually does not involve and is therefore distinguished from loss caused by physical harm. Our law traditionally afforded this kind of damage in the context of breach of contract, rather than in the law of delict.

---

[62] Visser P J and Potgieter J M *op cit* page 190
[63] *Administrateur, Natal v Trust Bank van Afrika Bpk* 1979 3 SA 824 (A)

Developments in our law have however opened the door to the awarding of compensation for pure economic loss also in regard to delictual liability.

One such area is liability for negligent misstatements or misrepresentations. Following upon the important English case of *Hedley Byrne v Heller [1964] AC 465 (HL)* our Appellate Division accepted in the case of *Administrateur, Natal v Trust Bank van Afrika Bpk*, that negligent misstatement causing pure economic loss can, in principle, give rise to delictual liability. In the case of *Bayer South Africa (Pty) Limited v Frost 1991 (4) SA 559 (A)* the Appellate Division also held that a negligent misrepresentation inducing a contract could similarly give rise to delictual liability. The factors to be taken into account quantifying the damages to be awarded were stated to be the following:-

(i) The policy limits of relying on the legal duty;
(ii) The professional standing of the maker of the misstatement;
(iii) The nature and interpretation of the misstatement;
(iv) The bounds of the test of negligence;
(v) Whether loss to the specific plaintiff was foreseen or foreseeable;
(vi) Causation; and
(vii) Curtailing the so-called "limitless liability" that could arise as a result of the awarding of damages.[64]

The advantage of being able to claim in delict rather than in contract, is that it entitles the plaintiff to a broader range of damages, such as general damages for pain and suffering. The fact that a plaintiff wishing to sue for pure economic loss arising from negligent breach of contract may elect to sue in delict was confirmed in the Appellate Division case of *Wassenaar & Partners v Pilkington Bros 1983 (1) SA 475 (A)*. In that case our Appellate Division confirmed that a plaintiff could, apart from the contractual claim for damages also elect to sue in delict, *provided that the independent requirements of delict are satisfied.*

[64] Burchell J, *The Odyssey of Pure Economic Loss*, University of Cape Town A*cta Juridica 2000,* edited by Scott T J, and Visser D, page 101

In assessing the liability to be visited upon negligent misstatements causing pure economic loss, various factors will be taken into account by our courts. An important consideration in the approach to negligent misstatements is the duty of care to be expected of professional persons as compared to the relative ignorance of clients and consumers. This is a factor that must be taken into account by long-term assurers when, during the course of transactions, financial advice is given to the client.

Another potential area of liability that long-term assurers must consider is the invasion of clients' rights of privacy. Included in a person's right to privacy is a person's right to decide *"when and under what conditions private facts (about the person) may be made public"*. The wide definition of "Personal Information" and the extent to which information regarding personal particulars of a client is obtained by a long-term assurer for purposes of issuing insurance contracts was pointed out above. Many of these particulars relate to what McQuoid-Mason refers to in an article that appeared in *Acta Juridica 2000* [65] as a "*person's inner sanctum"* as it relates to his or her family life, sexual preference and home environment. To this can be added sources of income, financial profile, dependants (which can include illegitimate children for which a policyholder secretly wants to provide) and medical status.

Traditionally our law recognised actions for the infringement of rights to privacy under the "*actio iniuriandi"*. With the adoption of South Africa's constitution in 1996 protection for a general right of privacy was introduced into our law. In particular, the right extends to the right of a person not to have:-

(a) His or her person home searched;
(b) His or her property searched;
(c) His or her possession seized; or
(d) The privacy of his or her communications interfered with.

[65]McQuoid-Mason D, *Invasion of Privacy: Common-Law v. Constitutional Delict – Does it make a difference?* Acta Juridica 2000, page 227

McQuoid-Mason considers the extent to which the constitutional protection given to privacy might create a constitutional action for damages and therefore a *"new delict"* as opposed to the common-law action merely *"subsuming"* the constitutional action.

The essential elements required for liability in terms of the common-law are the following:-

(i) An invasion of privacy;
(ii) Wrongfulness; and
(iii) Fault in the form of intention or *animus iniuriandi.*

The invasion of privacy can be constituted by an intrusion into privacy or the publication of private facts. Where private information about an individual is unlawfully published to third parties (without lawful justification) it could therefore give rise to an action for the invasion of privacy. The *"wrongfulness"* of the infringement of privacy in terms of the common-law is generally considered in terms of the *"boni mores"* of a society. It is an objective test in the sense that it will be measured against the ordinary or reasonable sensibilities of a society rather than *"hyper-sensitivity"*. Where an invasion of privacy therefore occurred regarding information that should not cause mental distress to a person of reasonable sensibilities such infringement will not be actionable.[66] Any court considering alleged invasions of privacy will also take into account some subjective factors relating to the circumstances of a particular case, such as the nature of the information and the personality and station in life of the plaintiff. McQuoid-Mason points out that such *"subjective-objective approach"* will be similar to the approach adopted by the Constitutional Court when it held that *"a person's subjective expectation of privacy will only have been wrongfully violated if the court is satisfied that such expectation was objectively reasonable"*[67].

[66] McQuoid-Mason *op cit* page 232
[67] *Ibid* page 232

The impact of the Constitution on the development of our common-law must also not be underestimated, according to McQuoid-Mason, as it plays an important part in defining the *boni mores* of society. In terms of the constitution an infringement on a person's right to privacy is *prima facie* unlawful.

A further important influence that the constitution could have on the common-law protection of the right to privacy is in respect of the requirement of fault, being *animus iniuriandi.* Traditionally, the common-law required a subjective intention to injure a person with knowledge of the wrongfulness of the act. McQuoid-Mason expresses the opinion that the constitutional protection granted to the right of privacy could be regarded as so fundamental and important in South Africa's new democratic society that strict liability could be visited upon infringements thereof.[68]

Some support for this proposition stated by McQuoid-Mason can be found in the Chapter in LAWSA dealing with fault liability.[69] The writers point out that the norms and values enshrined in the constitution (as developed by the Constitutional Court) not only serve as "*yardstick for determining whether old principles are still current, but also as a source and inspiration for developing new principles and rules*". It states that the Bill of Rights can even be considered as "*the fourth pillar upon which our law of delict rests come together with the* lex aqilia, *the* actio iniuriarum *and the remedy for pain and suffering*". In dealing with strict liability[70] the writers of LAWSA however point out that various attempts that have on occasion been made to introduce new instances of strict liability have so far not been successful. The liability of the mass media is cited as an example of an attempted introduction of strict liability that did not succeed. The writers also refer to our court's preference to extend liability rather by attenuated form of intention and reversal of onus of proof.

---

[68] McQuoid-Mason *op cit* page 234
[69] Law of South Africa, Second Edition, Volume 8(1), Delict, Liability in South African Law, Fault Liability, paragraph 23
[70] *Ibid* paragraph 28

The current reluctance of our courts to extend the protection of rights to privacy is somewhat surprising in light of a changing approach from a public point of view to the issue of privacy rights in the modern computerised and commercial world. Tapper[71] refers to "*five propositions*" in this regard. The first is the fact that we now live in a world where intrusions upon personal privacy are more common than ever before and increasing. The second relates to the fact that such intrusions can in part be blamed on the development of modern technology with specific reference to the application of computers for purposes of data processing which allows easy and instant access to vast quantities of information. The third is that although the information so stored is often inaccurate and unchecked, it is still regarded by its users as irrefutable evidence of whatever it represents. Fourthly, a general fear exists that information so stored will be available to any person who seeks to access it, whether authorised or unauthorised. Tapper identifies three elements relating to this proposition being:-

(i) the fear of unauthorised use by those to whom the information has been entrusted for some other purpose eg the compilation of a large personal dossier bringing together into one large file information about an individual;

(ii) the passing-on of personal information to third parties eg where a service bureau mixes up the files of different customers or where statistical information is released in a form from which personal information relating to individuals may be deducted; and

(iii) the fear that outsiders may break down the security of a computer system, either by suborning employees or by electronic invasion.

The fifth proposition relates to the absence of effective legal remedies to protect an individual whose privacy is threatened. This proposition and the criticism that it holds regarding current legal rules is, according to Tapper, based on a wrong assumption that developments in computer technology necessarily requires a corresponding development in legal rules. He points out that "*the criticism misconceives the nature of legal rules*"[72]

[71] Tapper *op cit* page 318
[72] *Ibid* page 322

and that judges should be more prepared to apply general principles to new situations. He interestingly also points out the absence of a general remedy in tort (delict) in the United Kingdom related to the protection of the right to privacy. He refers to the Younger Committee which was tasked to enquire into the desirability of establishing such a general remedy, but who rejected the idea.

Interestingly, the New Zealand Court of Appeal recently confirmed, according to an article written by Rosemary Tobin in the *LexisNexis Torts Law Journal*[73], a tort (delict) of *invasion of privacy* where private facts are published in circumstances where the publicity is highly offensive to an objective reasonable person.

In the article referred to above, McQuoid-Mason considers the extent to which the common-law of delict concerning personality rights should be incrementally developed in South Africa to accommodate constitutional protection of privacy or whether a new constitutional delict should emerge and if so, what it should look like.[74] From the outset he points out that a breach of s 14 of the Constitution will be regarded as *prima facie* proof of an unlawful invasion of privacy. It will shift the onus on the defendant to show that the breach was justified in terms of s 36 of the Constitution. He also points out that fault will not be a requirement and that the courts would have a discretion in awarding remedies. Unlike the common-law test for unlawful infringement of privacy, the test under the Constitution would be a "two-fold" enquiry comprising the following two questions:-

(a) Has the conduct complained of infringed the right to privacy as protected under the constitution; and

(b) Was the infringement justifiable in terms of the limitation clause.

In considering whether the action amounted to an infringement of the constitutional right to privacy, the court will firstly consider whether there was a *reasonable*

[73] Tobin R, *Yes, Virginia, there is a Santa Clause: the tort of invasion of privacy in New Zealand,* Torts Law Journal, May 2004 (2004 TLJ LEXIS 7).
[74] McQuoid-Mason *op cit* page 246

expectation of privacy. As stated above the plaintiff will have to show that he or she had a subjective expectation of privacy which was *objectively* reasonable. Although information therefore might pertain to the so-called *"inner sanctum"* of a person, that person's expectation of privacy must still be weighed up against *"the conflicting rights of the community"*.

In assessing whether an invasion of privacy occurred, a distinction must be made between several categories. Firstly there are the so-called *personal autonomy privacy cases* where protection is granted to individuals against intrusions and interferences with their *private lives*. Examples of such cases are the individuals' right to make personal decisions about this use such as their family relationships, home life and sexual orientation. The second category is *privacy rights protecting information.* These rights protect the gaining of access, publishing, disclosure or use of information about others without their consent. McQuoid-Mason also refers[75] to so-called "*special categories of privacy rights protecting information"* which includes unlawful searches of people's persons or homes and unlawful infringements of private communications.

As stated above fault is not a requirement for an action based on the infringement on a constitutional right to privacy. This is also referred to as *"strict liability"*. The remedies available to a plaintiff are:-

(a) constitutional damages;
(b) interdicts; and
(c) declarations of invalidity.

In cases for damages, the first two remedies will be of relevance. McQuoid-Mason points out that in awarding damages for delict resulting from breaches of constitutional fundamental rights our courts will in all probability be guided by the common-law and that it is unlikely that additional constitutional damages will be awarded unless it is regarded as "*an appropriate remedy"*. The common-law principles relating to damages

[75] McQuoid-Mason *op cit* page 250

in such a case are damages for patrimonial loss (if applicable), pain and suffering, loss of amenities (if applicable) and *contumelia.*

In the conclusion to his article McQuoid-Mason states as follows:-

> "*The courts will have to decide whether they wish to regard the common law delictual action for invasion of privacy or the constitutional right to privacy as the main vehicle for protecting individuals from unwanted intrusions or disclosures. For the present they seem content to develop the common-law by infusing it with the spirit of the constitution*"[76] and "*the emergence of a new constitutional delict would mean that a defendant could not rely on the usual delictual defences rebutting unlawfulness but would have to show that his or her conduct was reasonable and justifiable in terms of the limitation clause in the Constitution.*"[77]

Long-term assurers will be well advised to recognise the increasing protection that our courts give to litigants who prove that their rights to privacy have been violated. By virtue of the personal nature of long-term insurance contracts, long-term insurers are entrusted with confidential personal information pertaining to each policyholder. By inviting persons to enter into transactions for long-term policies online and by storing and communicating huge volumes of personal information electronically, insurers will always be at risk of violating the privacy rights of their clients, whether as a result of a technical failure of an information system or by reason of human error.

[76] McQuoid-Mason *op cit* page 260
[77] *Ibid* page 261

CONCLUSION

It cannot be denied that the fast growing and worldwide trend of doing business over the Internet will, before long, convince long-term assurers of the benefits of offering their products for sale online. Already many people prefer the convenience and comfort of doing their banking online, as well as purchasing many products such as books, CD's, photographic equipment or even groceries in this manner. A purchaser can access a particular website from the comfort and safety of his or her own personal computer at home, or from a lap-top computer whilst waiting to board a flight at an airport, or even from a hand-held device, that provides internet access, whilst lying on the beach. And he or she can do it at any time that suits, without having to make an appointment to see a sales agent or experiencing the inconvenience of visiting a bank or a shop.

Security measures in online transactions and communications have also developed to the extent that purchasers need not fear unduly that their confidential information, such as banking details or personal information, would fall into the wrong hands and cause them embarrassment, harm or loss.

In many respects long-term insurance products do not lend themselves ideally to be purchased online. They are complex in nature due to the fact that they call for long-term financial commitments with long-term financial implications. They require various elections to be made such as the type and extent of cover required or the term that the cover will be in force. There is also the need to provide medical and other information to the assurer, upon which underwriting can be done. Most purchasers might therefore prefer to receive some measure of financial advice before entering into a transaction for a long-term insurance product.

It is also clear that the long-term insurance industry is heavily regulated, with a strong emphasis on disclosure. A plethora of legislation and Codes each require a list of

disclosures to be made, to which must be added the disclosures in terms of the ECT Act, in case of online transactions. There are also the requirements relating to the identification and verification of purchasers and the reporting of suspicious transactions to law enforcement agencies. At the same time long-term assurers will be bound to increasing demands to respect the privacy of purchasers and to ensure that they have adequate measures in place to protect data collected from purchasers. Long-term assurers could also face new grounds of action in claims for damages, should errors occur in the processing of electronic transactions or if personal information is divulged to unauthorised third parties.

The electronic medium of communication and digital information technology, however, brings with it solutions to many of the challenges mentioned above. Through expert website design long-term assurers can ensure that detailed product information is brought to the attention of a prospective purchaser in a manner that is both informative and easy to understand. "Click-wrap" and "web-wrap" methods can be used to ensure that purchasers are made aware of important disclosures and terms, before continuing with a transaction. Purchasers can be offered the opportunity to review a transaction and to terminate it if they so wish.

Financial calculators could assist in illustrating expected returns on investments or the premiums to be paid for the amount of cover required. Websites could be programmed to pose all the pertinent questions and prompts needed to establish financial needs. Glossaries could explain the meaning of technical terms. In an interview with a personal financial adviser, the same purchaser might feel too embarrassed to admit that he or she does not understand certain terminology or that he or she wishes to reconsider or even terminate a transaction. In transacting on a website no such personal discomfort need not occur. A purchaser need also not be concerned about the commission payable to an intermediary or that the advice received from such intermediary might be influenced by possible commission considerations.

Websites could also be designed to allow policyholders to access their portfolios and personal records from time to time to update personal particulars or to request additional information or changes to their contracts. Websites could also provide valuable information on claims procedures and allow policyholders to process such claims online.

It is hoped that the legislator will desist from over-regulating all aspects of online transactions and, in particular, transactions for long-term insurance products. The proper design of websites offering online transactions for long-term insurance products will assist in showing the benefits of transacting in this manner and to satisfy the legislator that more stringent regulation is not required. This will hopefully stimulate the growth in the business of online transactions in the long-term insurance industry.

BIBLIOGRAPHY

LEGISLATION

1. The Long-term Insurance Act, 52 of 1998
2. The Electronic Communications and Transactions Act, 25 of 2002
3. The Financial Advisory and Intermediary Services Act, 37 of 2002
4. The Financial Services Board Act, 97 of 1990
5. The Financial Intelligence Centre Act, 38 of 2001
6. The Promotion of Access to Information Act, 2 of 2000

TEXTBOOKS

1. Hofman J, *Cyberlaw, a guide for South Africans doing business online*, Ampersand Press, 1999
2. Buys R et al, *Cyberlaw@SA II, The law of the Internet in South Africa*, Van Schaik, 2004
3. Christie R H, The Law of Contract, 4th Edition, Butterworths, 2001
4. Visser P J and Potgieter J M, *Law of Damages,* Juta and Company Limited, 1993
5. Harms L T C, *Amlers Precedents of Pleadings*, Butterworths, 4th Edition, 1993
6. Tapper C, *Computer Law* , Longman Group UK Ltd, 4th Edition, 1998
7. Boberg PQR, *The Law of Delict,* Juta and Company Ltd, 1984

ARTICLES

1. Brett J, *A Web Wake-Up Call*, Limra's Market Facts Quarterly / Fall 2005
2. Schofield S, and Davis York H, *FSR Impacts on Financial Services Technology*, New South Wales Society for Computers and the Law, Journal: December 2004, Issue 58

3. Lodge T and Kho R, *Online Transactions between Members and Borrowers – Proposed Changes to the Uniformed Consumer Credit Code*, New South Wales Society for Computer and the Law Journal : December 2004, Issue 58
4. Barnett P, *The Write Stuff? Recent developments in electronic signatures*, New South Wales Society for Computers and the Law, Journal : December 2001, Issue 46
5. Weitzenboeck E M, *International Journal of Law and IT*, September 2001, Oxford University Press
6. Burchell J, *The Odyssey of Pure Economic Loss*, University of Cape Town *Acta Juridica 2000* edited by Scott, T J and Visser, D,
7. McQuoid-Mason D, *Invasion of Privacy: Common-Law re Constitutional Delict – Does it make a difference?* Acta Juridica 2000
8. Tobin R, *Yes, Virginia, there is a Santa Clause: the tort of invasion of privacy in New Zealand*, Torts Law Journal, May 2004 (2004 TLJ LEXIS 7)

WEBSITES

1. http://searchsmb.techtarget.com/sDefinition/0,,sid44_gci211561,00.html
2. www.e.consultancy.com/publications/internet-stats-compendium
3. www.emarketer.com; http://retailindustry.about.com/library/bl/bl_em0320.htm
4. http://www.census.gov/mrts/www/ecomm.html
5. www.loa.co.za
6. www.uncitral.org/uncitral/en/uncitral-texts/electronic_commerce/1996Model.html
7. http://www.rsasecurity.com/rsalavs/node.asp?id=2157
8. http://www.webopedia.com/TERM/S/SSl.html
9. www.doj.gov.za/salrc/dpapers/
10. www.fsb.co.za

CASES

1. *Caspi v The Microsoft Network L.L.C.* Superior Court of New Jersey Appellate Division 323 N.J. Super.118; 732 A.2d 528; 1999 N.J.Super. Lexis 254 (July 2, 1999)
2. *Specht v Netscape Communications Corp*, 306 F.3D17 (2d CIR. 2002)
3. *Administrateur, Natal v Trust Bank van Afrika Bpk* 1979 3 SA 824 (A)